

In The Matter Of:
United States vs.
PFC Bradley E. Manning

Vol. 21
July 25, 2013
UNOFFICIAL DRAFT - 7/25/13 Morning Session

Provided by Freedom of the Press Foundation

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

VOLUME XXI

IN THE UNITED STATES ARMY

UNITED STATES

VS.

MANNING, Bradley E., PFC COURT-MARTIAL

U.S. Army, xxx-xx-9504

Headquarters and Headquarters Company,

U.S. Army Garrison,

Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

_____ /

The Hearing in the above-titled matter was

held on Thursday, July 25, 2013, at 9:30 a.m., at

Fort Meade, Maryland, before the Honorable Colonel

Denise Lind, Judge.

DISCLAIMER

This transcript was made by a court reporter who is not the official Government reporter, was not permitted to be in the actual courtroom where the proceedings took place, but in a media room listening to and watching live audio/video feed, not permitted to make an audio backup recording for editing purposes, and not having the ability to control the proceedings in order to produce an accurate verbatim transcript.

This unedited, uncertified draft transcript may contain court reporting outlines that are not translated, notes made by the reporter for editing purposes, misspelled terms and names, word combinations that do not make sense, and missing testimony or colloquy due to being inaudible by the reporter.

1 **APPEARANCES:**

2
3 **ON BEHALF OF GOVERNMENT:**

4 **MAJOR ASHDEN FEIN**

5 **CAPTAIN JOSEPH MORROW**

6 **CAPTAIN ANGEL OVERGAARD**

7 **CAPTAIN HUNTER WHYTE**

8 **CAPTAIN ALEXANDER van ELLEN**

9
10 **ON BEHALF OF ACCUSED:**

11 **DAVID COOMBS**

12 **CAPTAIN JOSHUA TOOMAN**

13 **MAJOR THOMAS HURLEY**

1 PROCEEDINGS,

2 THE COURT: Court is called to order.

3 Major Fein, please account for the parties.

4 MAJOR FEIN: Yes, Your Honor. All parties
5 when the Court last recessed are again present.

6 Captain Morrow is present and Captain Whyte is absent.

7 Additionally, Your Honor, as of 9:20 this
8 morning there are 54 members of the media at the Media
9 Operation Center, one stenographer, 8 members of the
10 media in the courtroom in the panel box, 35 spectators
11 in the courtroom and 14 spectators in the overflow
12 trailer.

13 Also, the alternate site other than the
14 chapel is available, if needed, because the overflow
15 trailer is not at maximum capacity, is not being
16 currently used.

17 THE COURT: All right. Thank you.

18 MAJOR FEIN: Also, the Court Reporter has
19 changed. Mr. Robert Shaw is absent. Mr. Chavez is
20 present.

21 THE COURT: All right. Have we had any

1 additional exhibits filed with the Court Reporter?

2 MAJOR FEIN: Yes, your Honor. Appellate
3 614, dated July 24, 2013, is a defense motion for
4 reconsideration and for mistrial for Specification 4,
5 6, 8, 12 and 16 of Charge 2, 18 USC 641 offenses.

6 Gollihood 615, dated 25 July 2013, is a
7 Government accounting of expert witness for
8 presentencing.

9 Appellate Exhibit 616, dated 25 July 2013
10 is the Government's schedule of witnesses for
11 presentencing phase. And also, Your Honor, Appellate
12 Exhibit 617 is a Government's classified supplement for
13 closing argument.

14 THE COURT: What was 616 again?

15 MAJOR FEIN: Your Honor, United States
16 schedule or proposed schedule for sentencing witnesses.

17 THE COURT: Mr. Coombs.

18 MR. COOMBS: Yes, Ma'am. With regard 614
19 our motion, the Defense would request ability to
20 publish that motion today on its website. I believe in
21 accordance with the Court's requirements the motion can

1 be published. I know the Government has a process
2 which anytime there is an appellate exhibit, it
3 ultimately get put on the FOIA reading room. However,
4 I would like to have the motion posted today.

5 THE COURT: Government, any objection?

6 MAJOR FEIN: Your Honor, so long as the
7 Court's order is being followed, no objection.

8 THE COURT: All right. That's fine, Mr.
9 Coombs.

10 All right. The Court, once again, is
11 prepared to rule on the Defense motions for Finding of
12 Not Guilty under Rules of Court Martial 917. The Court
13 ruled on this yesterday actually and gave the parties
14 an advanced copy of the ruling so they would be
15 prepared, either in closing argument today.

16 Last night Mr. Coombs sent by email a copy
17 of the Request for Reconsideration that he has filed.
18 And before I read the ruling, counsel and I met briefly
19 in an RCM 802 conference before we came on the record
20 today.

21 Once again, that is a conference where the

1 parties and Court discuss logistics and scheduling and
2 other issues that might arise in cases.

3 The Government will file a response to that
4 motion by tomorrow evening. And over the weekend Mr.
5 Coombs will advise the Court on whether or not the
6 Defense request oral argument on that motion. And we
7 have not scheduled oral argument for it yet --
8 actually, we will. If we have oral argument on that
9 motion, it will be Monday morning 0930.

10 (The Court read ruling)

11 Is there anything else we need to address
12 before we proceed to closing argument?

13 MR. COOMBS: If we could have a brief ten
14 minute conference break.

15 THE COURT: All right. Why don't we recess
16 the Court then until 10:45.

17 (Brief Recess)

18 THE COURT: Court is called to order.
19 Record reflect that all parties present when the Court
20 last recessed are again present.

21 Government, ready to proceed?

1 MAJOR FEIN: Yes, Your Honor.

2 Your Honor, if it may please the Court. In
3 late October 2009 Pfc Bradley Manning deployed with his
4 unit to a war zone, having sworn an oath of allegiance
5 in a place to protect national security interest of the
6 United States.

7 He deployed fully armed, not only with
8 protective gear and a rifle, but armed with the stark
9 knowledge of the harm that could accrue if classified
10 materials compromised.

11 His mission, as an all intelligence analyst
12 was a special trust. But within weeks of arriving at
13 Iraq, he abused and destroyed this trust with the
14 wholesale, indiscriminate compromise of hundreds of
15 thousands of classified documents.

16 He delivered these documents ready made for
17 use by an enemy via a platform he had long researched
18 and come to know, WickiLeaks. He delivered these
19 documents for notoriety.

20 Pfc Manning's state of mind has been
21 subject of speculation throughout this trial, Your

1 Honor. Yet humans dog tags couple with the fact of the
2 matter is that the only human Pfc Manning ever actually
3 cared about was himself and his carelessness is
4 revealed through his own chats.

5 If at the country, he got notoriety.
6 Worldwide anarchy in CSD format Hillary Clinton is
7 going to have a heart attack. And the best evidence of
8 Pfc Manning's state of mind before he had time to make
9 up a story is a picture, Your Honor. This picture, a
10 picture is worth a thousands words.

11 This picture was taken by Pfc Manning
12 himself in January of 2010, during the same week he
13 transmitted hundreds of thousands of Significant
14 Activity Reports to WikiLeaks. And this picture, Your
15 Honor, was found in the same SD card as those
16 classified SigActs.

17 What you see, Your Honor, in this picture
18 is not a troubled, anguished or well intentioned
19 soldier struggling with the consequences of U.S.
20 military action or foreign policy. This is a gleeful
21 grinning Pfc Manning, who signed the transmittal letter

1 to WikiLeaks describing the SigActs with the
2 salutation, have a good day.

3 Pfc Manning has been six months of a combat
4 deployment. Abusing his access is pertinent. Looking
5 for bigger fish, more damaging information to scrape
6 because he wasn't interested in oaths, or obligations
7 or simple acknowledgments that he would protect closely
8 held information.

9 He was interested in making a name for
10 himself. A statement he made prior to deployment
11 turned out actually to be true. The flag meant nothing
12 to him.

13 Pfc Manning was calculating and
14 self-interested. His acts resulted in the unfeathered
15 access to classified information by enemies of the
16 United States, an outcome all too clear to him as a
17 result of his training, Your Honor.

18 How did Pfc Manning know the enemy would
19 receive this information? He's aware of how WikiLeaks
20 operated and the type of information they sought. He
21 knew that what he provided to WikiLeaks, would make

1 its way to the enemy. Because he knew the enemy used
2 WikiLeaks as their own resource. Pfc Manning knew
3 that WikiLeaks, and specifically Julian Assange,
4 considered themselves the first intelligence agency for
5 the general public. Because it did quote from his
6 chats everything an intel agency does, end quote.

7 Pfc Manning scoured every possible source
8 about WikiLeaks he could find on SIPRnet, the
9 classified SIPRnet, and saw how the United States
10 Government intelligence community considered WikiLeaks
11 a threat to the United States, an organization with the
12 term leak in their name who specialized in assisting
13 those with access to classified information and
14 extracting that information from Government systems and
15 disclosing it to the world anonymously.

16 Your Honor, there's voluminous amounts of
17 evidence in this case. And United States is cognizant
18 the clear understanding of what Pfc Manning did or did
19 not do and what he did or did not know.

20 In order to best understand this complexity
21 of the evidence, the United States intends to follow

1 this roadmap for the remaining portion of the argument.

2 First, Your Honor, a recount of key
3 evidence. The United States intends to explain how Pfc
4 Manning's formal education and training gave him skills
5 and knowledge that he ultimately used to the detriment
6 of the United States.

7 Then, Your Honor, I intend to explain Pfc
8 Manning's work product as an intelligence analyst to
9 demonstrate how he knew and appreciated the types of
10 information he deliberately and intentionally chose to
11 compromise.

12 Then, Your Honor, I intend to explain Pfc
13 Manning's actual knowledge of WikiLeaks through his
14 own words and research, focusing on what Pfc Manning
15 knew and thought at the time he was actually
16 compromising information to WikiLeaks.

17 Then, Your Honor, I intend to walk you
18 through the evidence in a chronological order by type
19 of information that Pfc Manning intentionally and
20 deliberately compromised through multiple
21 transmissions. This, Your Honor, is the order that

1 will see.

2 Then, Your Honor, I'll outline the evidence
3 proving that Pfc Manning wantonly caused intelligence
4 to be published on the internet, conduct that was
5 prejudicial to good order and discipline and services
6 discredit to the armed forced.

7 Finally, Your Honor, I'll outline the
8 evidence that will prove that Pfc Manning aided the
9 enemy of United States by knowingly giving intelligence
10 through indirect means to al-Qaida and al-Qaida in the
11 Arabian Penninsula.

12 Throughout this case, Your Honor, the
13 United States admitted more than 160 pieces of physical
14 and documentary evidence. The Court has heard
15 testimony from more than 80 witnesses, including
16 stipulations of expected testimony and two stipulations
17 of fact.

18 Although all this evidence is useful to
19 understand how Private First Class Manning committed
20 his crimes, as it relates to specific specifications
21 and charges that are key pieces of evidence for which

1 United States explained during the opening that spent
2 more than one of the specifications. And the United
3 States argues that this evidence, this key evidence,
4 should remain in the forefront of your mind during
5 deliberations.

6 First, Your Honor, SIPRnet computers
7 identified as .22 and .40. These two SIPRnet computers
8 and the computers -- and it is his link to closely held
9 world maintained by an intelligence community on
10 SIPRnet.

11 Second, Pfc Manning's personal computer, an
12 Apple McIntosh laptop. This computer was Pfc Manning's
13 connection between the closely held war on SIPRnet and
14 his connection to the rest of the world. He used this
15 computer to communicate and transfer the closely held
16 information to Julian Assange's to WikiLeaks.

17 He also forensically wiped his computer on
18 31 January 2010, thus covering his tracks and deleting
19 any forensic evidence of his crimes prior to that date.

20 What Pfc Manning did not plan for, Your
21 Honor, was the ability of the forensic examiners to

1 recover certain information such as the chats between
2 him as Julian Assange and Adrian Loma and the volume
3 mounting data.

4 The volume data shows the date that certain
5 information was burned on the CDs from his SIPRnet
6 computer and the CDs brought into and introduced by
7 Personal Mac. That information was logged as a key
8 piece of evidence in this case.

9 Third, Your Honor, Pfc Manning's external
10 hard drive. This is an external storage device that he
11 brought to Iraq with him to store contact information
12 for WickiLeaks, army doctrine and training, his own
13 corrected training offset briefing, which I'll discuss
14 later.

15 Fourth, Pfc Manning's SD card, on which he
16 saved a copy of the entire SigAct portion of CIDNI Iraq
17 and Afghanistan databases as a trophy for successful
18 disclosures.

19 Fifth, J.C. Katz's computer from Brook
20 Haven National Laboratories, which contained the Garani
21 airstrike video compromised by Pfc Manning in a file

1 dated 15 December, 2009. 15 December 2009, Your Honor.

2 The sixth key piece of evidence are the
3 audit logs. These are from multiple servers, firewalls
4 operating on SIPRnet, which captured Pfc Manning's
5 minute-by-minute activity across the classified web.
6 Intel link logs that show searches for WikiLeaks 119
7 times during 1 December 2009, two weeks, Your Honor,
8 after having access to SIPRnet.

9 The same time SharePoint server logs
10 showing the (inaudible) investigation being accessed.
11 Department of State server and firewall logs showing
12 amounts of data and activity in the late March and
13 early April 2010 timeframe. The Sidtar net flow data
14 logs that show Pfc Manning crisscrossing across the
15 SIPRnet connecting a different service to his two
16 SIPRnet computers.

17 Your Honor, seven, the computer with the IP
18 address ending .19. This is the computer Pfc Manning
19 used to steal USFI Global Access List.

20 The eighth piece of key evidence, Your
21 Honor, Prosecution Exhibit 130. Your Honor,

1 Prosecution Exhibit 130 is the evidence showing Pfc
2 Manning elicited Julian Assange to assist him in
3 cracking a password, a user password on a SIPRnet
4 computer. And finally, Your Honor the WikiLeaks Most
5 Wanted List, Pfc Manning's guiding light on what
6 SIPRnet available information he should target for
7 release.

8 Your Honor, as previously stated, Pfc
9 Manning is and was at the time an all source
10 intelligence analyst. He was granted SIPRnet access to
11 accomplish his duties and responsibilities as an
12 intelligence analyst.

13 He received a full compliment of training
14 for 35 to AIT. Multiple witnesses testified that Pfc
15 Manning was AIT attended every class that they could
16 remember, received formal training presented in
17 Prosecution Exhibit 5 and Prosecution Exhibit 6. Your
18 Honor, those are the program instruction lesson plans
19 and AIT student evaluation plan.

20 Your Honor, in terms of information
21 security. Specifically information security. Pfc

1 Manning received a briefing that's at Prosecution
2 Exhibit 52. That's this slide. This is Slide 1. The
3 actual training Pfc Manning received on information
4 security Army Regulation 380-5.

5 Slide 7, Your Honor, the classification
6 designations. What information was confidential,
7 secret, top secret, what does it mean when something is
8 secret or confidential. That it can cause serious
9 damage to national security.

10 Slide 8, Your Honor, the process of
11 classifying information. How do the United States
12 Government, under the Executive Order and Army
13 Regulations classify who are the proper authorities and
14 who is allowed to make those decisions.

15 Your Honor, Slide 10. The criterion
16 classified information. What type of information is
17 classified when you see a classified document from
18 military plans and weapon systems to foreign relations.

19 Slide 11, Your Honor, the prohibitions and
20 limitations. And the key here is in the blue on the
21 bottom where Pfc Manning was put on notice that

1 classified information is owned by and produced by and
2 is under the control of the United States Government.

3 Your Honor, Slide 14, Pfc Manning learned
4 how to properly mark documents and read documents and
5 know if they are marked classified.

6 Slide 21. He learned about the
7 declassification process; who are the authorities; who
8 is allowed to let information out of the possession of
9 the United States Government.

10 Slide 31. He specifically learned about
11 individual responsibility. His responsibility to
12 protect classified information.

13 Slide 38. The different way to store
14 classified information, the standards and regulation.

15 And Slide 41, the control measures in place
16 in order to protect classified information.

17 Your Honor, during the briefing he also
18 learned under Slide 48 how to properly mark digital
19 media with the different types of stickers, if it's
20 secret, top secret, unclassified or confidential.

21 We know Pfc Manning understood how to label

1 digital media in this case. You heard Special Agent
2 Smith that he found the Apache video on a disk in Pfc
3 Manning's shoe on a secret sticker. This is it, Your
4 Honor, Prosecution Exhibit 15. A secret sticker that
5 Pfc Manning put on the CD because he believed at the
6 time, even though he burned it from his personal
7 Macintosh computer that that video, the Apache video
8 was classified secret.

9 Your Honor, according to Prosecution
10 Exhibit 52, Private First Class Manning was trained
11 also on why it was important to protect particular
12 information. So here is Slide 71. The enemy will
13 attempt to discover how and when we are conducting
14 operations. Knowing this we must protect our
15 activities from detection.

16 Slide 72. The critical information we
17 protect from enemies. (Inaudible)

18 Finally, Your Honor, Slide 73. The reason
19 we prevent disclosures in bright bold red. Don't
20 discuss operational activities on the web or email.
21 Consider the audience when you are posting to a blog,

1 personal web page or an email. Always assume the
2 adversary is reading your material. And at bottom,
3 remember, it's called the worldwide web for a reason.

4 This is the training he received day one as
5 an intelligence analyst.

6 What slide you did not see in the slide
7 deck presented in Prosecution Exhibit 52 for the entire
8 set of slides, the slide that tells Pfc Manning that
9 he's authorized to make classification decisions. He's
10 authorized to disclose information he chooses to, to
11 foreign nationals and ultimately to enemies of the
12 United States.

13 Your Honor, Mr. Mole, Pfc Manning's AIT
14 instructor recounted that, when instructing Pfc Manning
15 in his class, he explained that the worldwide web was
16 called that for a reason. Anyone had access to the
17 information on the internet and can see any of the
18 information that is on the internet. It was imperative
19 that soldiers understood this.

20 Mr. Mole taught Pfc Manning that whenever
21 they put information on the internet that it could be

1 used against them or against the U.S. military. And he
2 talked the following example, his own words, to the
3 lowest level of how posting information how it could
4 help the enemy, if given soldier's name, mother's
5 maiden name and social security number, filed separate
6 as an example couldn't do much damage.

7 But he explained to the lowest level, when
8 that information is combined, and that is put on the
9 internet, that a person could grab that information,
10 take credit out of someone's name and do harm to that
11 individual and that individual's reputation.

12 Similarly, he taught Pfc Manning, if you
13 release a unit's name, their location and mission then
14 the enemy can use that information to plan an attack on
15 our units.

16 Your Honor, Pfc Manning was trained on the
17 identities of terrorist groups, including al-Qaida,
18 using training slides from AIT, Prosecution Exhibit 51,
19 Mr. Mole testified that Pfc Manning was trained the
20 enemy used the internet. And that anything that the
21 enemy can use or piece together to use against the

1 United States should be protected, to include PPI, unit
2 identification and movement information.

3 Mr. Mole also instructed Pfc Manning on
4 specific enemies and what capabilities. He taught Pfc
5 Manning about terrorism and different terrorist
6 organizations.

7 Slide 216, Your Honor, Pfc Manning formally
8 learned who al-Qaida was and specifically who Osama bin
9 Laden was.

10 Slide 219, formally learned who al-Qaida in
11 Iraq was. Slide 221, learned about the recruiting that
12 terrorists did.

13 Slide 223, Pfc Manning learned that over
14 the past 10 years the number of terrorist websites has
15 jumped from less than 100 to as many as 4,000.

16 In addition to this training, Your Honor,
17 the United States admitted Pfc Manning's information
18 assurance training and certificates that showed he
19 completed that training. Prosecution Exhibit 7 and
20 Prosecution Exhibit 114.

21 Your Honor, Prosecution Exhibit 7 the

1 training that he received in 2008 and 2009. Slide 2,
2 based off this training he knew each and every one of
3 us play a vital role in DoD information safe and must
4 abide by the principles of IA in a daily routine and
5 protect the OB information in our systems.

6 Your Honor, Slide 7 of the training that he
7 passed the test twice on. Pfc Manning knew the
8 importance of critical infrastructure protection, that
9 if information and information systems are compromised,
10 it can impact our mission or national security and
11 ultimately our lives.

12 Your Honor, Slide 11. Prosecution Exhibit
13 7. Pfc Manning knew the threats made to information
14 assurance, which included both internal and external
15 human threats, specifically disgruntled employees,
16 spies or terrorists and hackers.

17 Your Honor, as a trained intelligence
18 analyst, Pfc Manning was required to have a secret
19 clearance AIT and eventually top secret SCI clearance
20 as a full 35 Fox.

21 Pfc Manning knew that a person may only be

1 granted access to classified information if three
2 things were true; first, the individual has a security
3 clearance; two, individual has a need to know the
4 information; and three, the person has signed a
5 nondisclosure agreement, SF?12.

6 Pfc Manning signed on two separate
7 nondisclosure agreements and a litany of other
8 acknowledgments. These documents permitted him to have
9 access to classified information, identified the
10 information that was owned by the United States
11 Government, highlighted potential ramification to
12 disclose or handle classified information improperly
13 and what a soldier is required to do if he is uncertain
14 of the classification status of the information. A
15 document signed, two documents, signed by Pfc Manning
16 on what he is required to do, if he's uncertain about
17 classification.

18 A violation of nondisclosure agreements can
19 result in criminal prosecution under 18 U.S.C. 7-903
20 and 641.

21 Your Honor, Elisa Ivory, she testified

1 through a stipulation of expected testimony that on 7
2 April, 2008, she briefed Pfc Manning about the dangers
3 of putting U.S. Army and Government classified
4 information on the internet.

5 She briefed Pfc Manning that putting
6 information on the internet not only exposes
7 information related to our national security, but it
8 also puts each soldier with a security clearance at
9 risk of black mail by our adversaries given their
10 position of trust to safeguard classified information.

11 Ms. Ivory also explained to Pfc Manning the
12 purpose of the NDA. And it asked Pfc Manning if he
13 wanted to voluntarily sign that. He did. Then Pfc
14 Manning stood, raised his right hand and stated that he
15 accepted the responsibilities contained within that
16 nondisclosure agreement. Including that he accepted
17 the special confidence and trust placed in him by
18 United States Government. Pfc Manning then executed
19 that NDA with Ms. Ivory.

20 Prosecution Exhibit 59 is that
21 nondisclosure agreement, which Pfc Manning pledged not

1 to violate in order to obtain access to classified
2 information.

3 Now, Your Honor, Prosecution Exhibit 60 is
4 a second nondisclosure agreement, which Pfc Manning
5 pledged not to violate in order to obtain classified
6 information while at 210 Mountain. And Chief Balonek
7 made sure he understood those obligation, as he
8 testified.

9 Your Honor, by voluntarily signing two
10 nondisclosure agreements, he knew the importance of
11 protecting classified information and that the
12 violations of the agreements could result in the
13 precise criminal action of this trial.

14 Pfc Manning knowingly violated both
15 nondisclosure agreements; thus, violating the special
16 trust and confidence that he committed to in order to
17 obtain access to classified information. That same
18 access that he abused in order to disclose hundreds of
19 thousands of classified documents.

20 Your Honor, during AIT Pfc Manning learned
21 and understood how the United States Army and its

1 enemies waged war. This is evidenced by the amount of
2 training materials that Pfc Manning himself retained
3 and cataloged on his external hard drive, Prosecution
4 Exhibit 11.

5 Your Honor, what did Pfc Manning keep for
6 easy reference next to the WikiLeaks contact
7 information file, that's Prosecution Exhibit 24, talk
8 about a moment.

9 He kept the Microsoft PowerPoint Brief
10 Title Insurgent Propaganda TTPs. He kept a copy of
11 U.S. Army Field Manual 2-0 titled Intelligence, which
12 states that our enemies weapons range from computers
13 connected to the internet to weapons of mass
14 destruction.

15 He kept a copy of Army Regulation 525-13
16 entitled Anti-Terrorism. That regulation states that
17 terrorists use instances of website tampering to
18 further their cause.

19 He kept on his external hard drive a copy
20 of U.S. Army Field Manual 7-100.1, which states that
21 personal computers on the internet are few examples,

1 just a few, of the capabilities widely available to
2 nations, independent organizations and individuals.
3 Met the information warfare could be conducted with
4 such easily accessible means such as the internet.

5 He also kept a copy of Army field Manual
6 7-100.4, which in Appendix C states, that the insurgent
7 organizations may be capable of cyber mining for
8 intelligence.

9 Your Honor, Pfc Manning neatly organized
10 possession of all this information on his exsternal
11 hard drive. That is additional evidence he knew and
12 understood all that information.

13 He showed that he had actual knowledge by
14 enabling closely held information, information he
15 posted on the internet. He was given that information
16 that enemies of United States and specifically al-Qaida
17 and al-Qaida in the Arabian Peninsula.

18 In addition to AIT training and reference
19 material Pfc Manning saved on his external hard drive,
20 he received formal and on-the-job training as
21 intelligence analyst.

1 Your Honor, according to Sergeant First
2 Class Emeker at his first JRTC rotation, Pfc Manning's
3 job was focused on signature activities in areas of
4 operations. This required constant research, constant
5 reviewing of information related to attacks that
6 insurgents were conducting, such as with IEDs, small
7 arms fire, indirect fire.

8 Pfc Manning was required to pull that
9 information and put together timelines for the S2 shot.
10 When IEDs were occurring and how often and where. So
11 the other analysts could go patten analyses product to
12 see if the IEDs could be targeted.

13 The intelligence Pfc Manning mined was
14 actually SigActs. Chief Balonek also testified he
15 trained Pfc Manning on how to use D6A machine in data
16 mining. Chief Balonek testified that he worked with
17 Pfc Manning on intelligence summaries of the day, which
18 were a daily rule of all the intelligence reporting
19 from that day compiled into one document. And each
20 analyst, like Pfc Manning, was required to actually tag
21 it and give the meaning of those reports.

1 Your Honor, Mr. Madaras, then Sgt. Madaras,
2 testified that at his D6A training, Pfc Manning was
3 told that D6A field support representative would be
4 down range and be responsible for handling all hardware
5 and all software issues for the D6A machines in
6 theater. That is when Pfc Manning was first put on
7 notice that the D6A contractors were in charge of those
8 computers.

9 Sergeant First Class Anika testified Pfc
10 Manning had exposure to SigAct at Ft. Drum, not just at
11 JRTC. He is required to read reports, pick up the
12 highlights, locate the bad guys and brief those
13 findings. To the S2 and ultimately to the brigade
14 commander, Colonel Miller.

15 Sergeant first-class Anika testified that
16 Pfc Manning also read many intelligence summaries,
17 which included SigActs from the CIDNE database,
18 particular view from borne IED, assessment on pattern
19 analysis, assessments of the enemy in the area,
20 political figures that were friendly.

21 He also testified that the unit received

1 formal IED training in December of 2008. A mobile
2 training team, Your Honor, from the joint IED defeat
3 organization came to Ft. Drum to teach the analysts
4 what their organization did for units downrange and
5 where to go for assistance when finding IED cells in
6 certain area.

7 According to Mr. Madaras the unit trained
8 again in approximately July of 2009, at this time the
9 focus was on Iraq. During this second rotation Pfc
10 Manning was again assigned to fusion cell and similar
11 responsibilities as the previous JRTC.

12 Your Honor, it's clear that Pfc Manning
13 arrived at FOB Hammer with specialized training from
14 AIT, experience from two JRTC rotations and his
15 garrison intelligence work. He also arrived with an
16 external hard drive full of valuable and informative
17 intelligence references.

18 All this combined, Your Honor, all this
19 combined is enough to prove that Pfc Manning's actual
20 knowledge that the enemies of the United States used
21 the internet and WickiLeaks to gather information to be

1 used against this country.

2 However, Your Honor, there is one key piece
3 of evidence which Pfc Manning also brought to Iraq with
4 him that proves he should be held accountable for
5 deliberate and intentional acts of releasing volumes of
6 classified information through WikiLeaks to enemies of
7 this country.

8 We are here today, Your Honor, to hold Pfc
9 Manning accountable for the exact training he gave
10 others, the training he gave others on this subject
11 matter.

12 During Mr. Johnson's forensic examination
13 of Pfc Manning's external hard drive, he found Pfc
14 Manning's corrective training presentation, which
15 Sergeant Madrid confirmed was the one presented to him
16 by Pfc Manning. Your Honor, this is Prosecution
17 Exhibit 25.

18 Prosecution Exhibit 25, Slide 1, dated 13
19 June 2008, created, researched by, well then, Pv2
20 Manning, Bradley.

21 Your Honor, Slide 2, provides a roadmap to

1 protecting this country operational security. Slide 3,
2 Your Honor, Pfc Manning's definition of OPSEC focused
3 on the protection of information, public assets,
4 military assets, personnel and national security.

5 Slide 4, Your Honor, the type of
6 information to protect to include dates, times,
7 locations along also for official use only information,
8 such as the Army's capabilities on the battlefield.

9 Your Honor, Slide 5 of Pfc Manning's own
10 briefing where he's highlighting that you must protect
11 dates and kind of large groups within the Department of
12 Defense, high ranking NCOs, and even diplomats, protect
13 their information, Your Honor.

14 Slide 6, protecting location of Government
15 facilities and military installations. Slide 7.
16 Protecting individual soldier's names, family members,
17 dates of birth and addresses.

18 He recognized, Your Honor, that in Slide 7
19 soldiers are required to protect the names and other
20 identifying information of our fellow soldiers.

21 Slide 8. That we must protect the methods

1 of intelligence gathering, description of weapons and
2 vehicles we use, and the capabilities of the United
3 States Army.

4 9, Pfc Manning specifically lists those
5 groups that he didn't consider adversaries of the
6 United States for the purpose of divulging closely held
7 information, foreign governments, terrorists and anyone
8 including activists and hackers.

9 Slide 10, Your Honor. On 13 June 2008,
10 after identifying the adversaries to the United States
11 Pfc Manning further delineated the common OPSEC leaks
12 for closely held information. That includes on
13 newspapers and magazines, news programs and
14 documentaries and the internet. Including chatrooms,
15 social networking and videos.

16 And then on Slide 11, Your Honor, his
17 conclusion on 13 June, 2008, he concluded his briefing
18 by stating, soldiers must avoid disclosures of
19 information the following forms; public conversations
20 with journalists, posting information on the internet.
21 Soldiers must use common sense with OPSEC and protect

1 our nation's secrets. Because there are many enemies
2 and we live in a free and open society.

3 Your Honor, this is not the product of just
4 any soldier in uniform but of Pfc Manning, a trained
5 intelligence analyst who on 13 June 2008 understood
6 what he taught others that the importance of protecting
7 our closely held information and knew that releasing
8 such information on the internet would be in the hands
9 of terrorists and other adversaries of this nation.

10 Your Honor, Pfc Manning was an intelligence
11 analyst, as you know, assigned to the S2 Section at 210
12 Mountain. At FOB Hammer S2 Section worked in a T-SCIF
13 located in the brigade headquarter's building. The
14 T-SCIF was a facility designed to store classified
15 information.

16 Everyone who worked the T-SCIF was required
17 to have a top secret clearance. For requested access
18 required to have an escort to enter the SCIF. That
19 even included the brigade commander, Colonel Miller.

20 If the soldier did not have a security
21 clearance, the T-SCIF would be sanitized, each S2

1 solider, including Pfc Manning, was responsible for
2 moving classified information out of sight.

3 When a soldier entered or left the T-SCIF
4 they are not searched. Instead it was their personal
5 responsibility to leave any electronic devices outside
6 the SCIF and not to remove any classified information
7 from the SCIF unless for official purposes only.

8 Your Honor, why were soldiers not searched?
9 Captain Lim gave that answer. He testified with the S2
10 section trust. Trust was imperative because the
11 intelligence soldiers dealt with classified information
12 on a daily basis and it was their job, their specific
13 job to protect classified information.

14 Colonel (inaudible) testified that trust
15 within a unit is everything. It is no different as
16 infantryman to trust another soldier to provide front,
17 rear and side security on a convoy as it is for an
18 intelligence analyst who trusts his fellow analyst to
19 safeguard classified information from the hands of the
20 enemy.

21 If Pfc Manning had not signed those NDAs

1 before he was deployed, he would not have worked in a
2 T-SCIF and would not have been able to commit the
3 crimes we are here today for.

4 Your Honor, you have heard from a number of
5 witnesses about the jobs of an intelligence analyst in
6 deployed environment. In Pfc Manning's unit discussed
7 what systems were used, how intelligence products were
8 created and how to defeat the enemy, and what role Pfc
9 Manning specifically played in that process.

10 Your Honor, first, let's talk about what
11 system the analyst used at FOB Hammer. Intelligence
12 analysts at FOB Hammer primarily used the SIPRnet to
13 gather intelligence.

14 From SIPRnet the analysts were assigned a
15 D6A computer system, get programs D6A computers
16 contained program that were regularly used by the
17 analysts and readily accessible a special suite of
18 programs installed in the SIPRnet computers designed
19 for United States Army all source intelligence analyst
20 to complete their assigned task.

21 Your Honor, you heard from Sergeant Sadler,

1 a SIGIT solider, not an all source intelligence
2 solider, who never even that was a system solely for
3 all source intelligence analyst.

4 Mr. Kits testified that the D6A machine is
5 essentially for intelligence processing and
6 exploitation and dissemination capabilities. Members
7 of S2 section had complied with the programs commonly
8 employed by analysts within the office were CIDNE
9 (inaudible)

10 (inaudible) Your Honor, commonly used
11 system and database for analysts. In particular
12 analysts regularly SigActs which are tactical reports
13 significant activity from the field.

14 Your Honor, Mr. Buchanan, through a
15 stipulation of expected testimony testified that
16 Intelink is a search engine or SIPRnet similar to
17 Google, that also enables collaboration among members
18 of the intelligence community.

19 Mr. Madaras explained that analysts
20 typically used Intelink when they didn't have specific
21 background knowledge on a certain topic so they didn't

1 know what database to go to originally. So they would
2 search on Intelink.

3 Analysts also used other programs, such as
4 WorkChat, which is a collaboration tool, similar to
5 instant messaging, which allows analysts to quickly
6 receive and disseminate information to and from the
7 field up and down from the division to battalion.

8 Your Honor, you heard testimony how
9 analysts create their products. And Pfc Manning's role
10 in that process. Pfc Manning was assigned to the
11 fusion cell at FOG Hammer where he was responsible for
12 contributing to the large scale enemy train analysis
13 and predictive analysis focused on the Shia, his focus
14 in Southeast Baghdad Shia --

15 Your Honor, before continuing about the
16 steps that Pfc Manning went through in order to
17 accomplish his normal intelligence and show his
18 knowledge of what intelligence analysts knew about the
19 enemy, please note that the suite of tools that the
20 Army gave Pfc Manning to enable him to collate data,
21 those tools, that based on Pfc Manning's actions he

1 enabled the enemy to have that information that the
2 United States relies on its special tools to collate
3 organize and analyze.

4 He provided that information, packaged to
5 the enemy. So now they can just analyze. He took all
6 of the initial steps that they would need to do and
7 gave that to them packaged, ready to be exploited, and
8 the entire world. Yet we, United States Army, has
9 special systems that allows to pull that information.

10 So speaking of those systems, Your Honor,
11 the first step in the process is to pull and
12 consolidate from various sources a particular topic,
13 such as enemy activity in a region over a certain
14 period of time.

15 After organizing the information the
16 analysts would then plot the information on a map to
17 visualize or create an intelligence summary.

18 Members of Pfc Manning's unit testified
19 that he was the go-to-guy for data mining, the process
20 of gathering mass intelligence on a particular topic
21 and organizing that intelligence in a usable format.

1 Pfc Manning's job was to reach into foreign
2 databases, pull and organize it. He was ranked 10 out
3 of 10 in data mining. Captain Fulton and Chief
4 (inaudible) they testified in conducting this analysis
5 generally required (inaudible) to come databases for
6 the applicable SigActs.

7 Captain Fulton testified that often
8 employed Pfc Manning to data mine for mass information,
9 particularly the SigActs relating to specific enemy
10 activity, organize and display it on a map for her.

11 The purpose of this task, as Captain Fulton
12 explained, was to determine whether the amount of
13 attacks had increased or decreased over a time. As the
14 unit prepared to draw down and redeploy from Iraq.
15 Fulton used this information to brief Colonel Miller on
16 a weekly basis to make command decisions.

17 Chief (inaudible) testified that Pfc
18 Manning employed similar skills, so much so that he
19 prepared Iraq SigActs spanning a three year period in
20 IEDs, small arm fire against convoys and their brigade.

21 The second step in this intelligence

1 analyst product, process. As Chief Ehresman explained,
2 was to make an assessment on the current inbound threat
3 or may happen in the immediate or distant future. The
4 second step is where the analysis comes in to play;
5 mainly enemy trend analysis and predictive analysis.

6 Enemy trend analysis is a study of how our
7 enemies operate, to identify any trends or patterns in
8 their behavior. Predictive analysis is the art of
9 predicting enemy activity. Enemy activity based upon
10 enemy trends. Or put another way, enemy trend analysis
11 leads to predictive analysis.

12 Chief Ehresman testified that historical
13 and current data are important for conducting this
14 analysis, as enemy groups tend to operate in the same
15 areas and employ the same tactics over time.
16 Historical information is just as useful intelligence
17 analyst as the most current information.

18 It benefits -- it benefit, the historic
19 information versus current, varies based of the desired
20 intelligence product. The focus of the product.

21 Both enemy trend analysis and predictive

1 analysis is essential for the commander to make his
2 tactical decisions.

3 And you heard from Captain Fulton that Pfc
4 Manning was a good analysts and accomplished his
5 assigned tasks, which included pulling information
6 based on his knowledge of what the officer, she wanted
7 or needed about the enemy.

8 You also heard from Mr. Hall, a defense
9 expert qualified in the field of intelligence analyst,
10 even junior analyst, like Pfc Manning, knew that the
11 enemy's capability and the enemy is just as capable as
12 piecing together information as our own junior analysts
13 are.

14 Although junior analysts are not expected
15 to that in-depth predictive analysis, they understand
16 the enemy's capabilities to use that information.

17 Your Honor, you also heard from Mr. Hall
18 that all analysts understand PIR, priority information
19 requirements. The gaps in intelligence information
20 that a commander has about the enemy, and how
21 intelligence analysts know this and work to answer

1 those specific gaps.

2 Your Honor, Pfc Manning was a trained
3 analyst who understood how to assess the enemy and how
4 the enemy assesses U.S. Forces deployed.

5 Although not a senior analyst, Pfc Manning
6 pulled data and conducted analysis to assist the senior
7 analysts with making actionable conclusions. He was
8 specifically trained on how the enemy also conducted
9 its own analysis and their capabilities to use
10 information about U.S. forces and the United States
11 national security and then fight against the United
12 States.

13 Your Honor, Pfc Manning's knowledge of and
14 relationship with WikiLeaks, including when that
15 relationship began, is readily apparent when all the
16 evidence is considered together.

17 What is obvious is that Pfc Manning pulled
18 as much information as possible to please Julian
19 Assange in order to get that information released and
20 Julian Assange found the right insider to mind SIPRnet
21 and the NIPRnet databases.

1 Pfc Manning began data mining of SIPRnet
2 for intelligence relating to WikiLeaks organization
3 soon after arriving in theater. Or more precisely,
4 Your Honor, using his own words, right after
5 Thanksgiving timeframe of 2009. Those Lamo chats, Page
6 9.

7 Your Honor, Prosecution Exhibit 24.
8 Mr. Johnson found the, forensically found a file
9 containing the contact information for Julian Assange
10 and WikiLeaks, the leader of WikiLeaks, on Pfc
11 Manning's external hard drive. This is the contact
12 information, Your Honor.

13 According to Mr. Johnson that file was
14 created on 29 November '09. 29 November '09. That is
15 less than two weeks after having access to SIPRnet that
16 Pfc Manning then began using his SIPRnet access to
17 search Intelink for WikiLeaks.

18 We have heard testimony, Your Honor, that
19 3rd Brigade, 2nd Airborne finished the rip total with
20 210 Mountain in second week of November. Which means
21 by the beginning of December, that is the first two

1 weeks that Pfc Manning had access to SIPRnet without
2 another soldier sitting to his left or right during the
3 (inaudible)

4 Your Honor, Special Agnet Shaver testified
5 that Pfc Manning searched Intelinks for the term
6 WickiLeaks more than 100 times beginning on 1
7 December 2009. Pfc Manning also searched for Iceland
8 related topics 25 times between January and April 2010.
9 And ample searched for Julian Assange in the same
10 timeframe.

11 You can see all the searches for WickiLeaks
12 on Prosecution Exhibit 81. Prosecution Exhibit 81,
13 Your Honor, is the summary of searches conduct by Pfc
14 Manning from his SIPRnet computer.

15 And according to Prosecution Exhibit 81, he
16 conducted four searches for the term WickiLeaks, Your
17 Honor, for approximately every five days that he was at
18 FOB Hammer. Four searches for the term WickiLeaks
19 every five days, when he was at FOB Hammer.

20 Your Honor, one day after returning from
21 R&R leave Private First Class Manning compromised

1 (inaudible) and other Department of State information.
2 WikiLeaks published the cable a day later. In
3 response to the public release of that cable by
4 WikiLeaks, Private First Class Manning observed that
5 the United States Ambassador to Iceland was recalled or
6 as he put it coldly, fired. That is in the Julian
7 Assange chat, Your Honor.

8 Your Honor, why would Pfc Manning be
9 searching for and so focused on Iceland as an United
10 States Army analyst focused on Southeast Baghdad,
11 deployed in Iraq. Iceland searches relate back to
12 Julian Assange, who was in Iceland in February 2010 and
13 working on Islandic Modern Media Initiative.

14 Pfc Manning knew that WikiLeaks would be
15 interested in matters pertaining to Iceland. That
16 could guarantee him real time disclosures actually on
17 the web, as fast as possible, for the world to access.

18 Your Honor, you heard evidence that Pfc
19 Manning used other sources on the SIPRnet to gather
20 information on WikiLeaks as well. Just five days
21 after returning from R&R leave Pfc Manning created an

1 Open Source Center account on 20 February 2010. And he
2 used the same moniker, BradS87 that he used in his Lamo
3 chats. Prosecution Exhibit 139 showed this
4 information.

5 Shaver testified that the same day Pfc
6 Manning began using is OSC account to search for terms
7 like WickiLeaks in Iceland. Mr. Allen testified that
8 the Open Source Center with a website (inaudible)
9 Central Intelligence Agency containing reports,
10 translation and other information on unclassified
11 publications worldwide. But it is not just a website
12 providing news updates. Special Agent Shaver testified
13 that Pfc Manning searched for WickiLeaks at OSC more
14 than 20 times. And information on Iceland more than 25
15 times. Your Honor, why else would Pfc Manning actively
16 seek a new account on the Open Source Center.

17 Julian Assange and Pfc Manning discussed
18 the Open Source Center what is available. Julian
19 Assange stated that the OSC is, something we want to
20 mine entirely. That is the Julian Assange chats, Page
21 5.

1 WickiLeaks' interest in the Open Source
2 Center and Government analysis is also confirmed by
3 Most Wanted List, Prosecution Exhibit 109. Both
4 databases.

5 Defense corresponding exhibit. So what did
6 Pfc Manning learn about WickiLeaks through all these
7 constant searches? The United States Government,
8 specifically United States military, created three
9 classified U.S. Government reports that focused on the
10 threat WickiLeaks poses to the national security, of
11 the United States; ASig report, NCIS IRR and the C3
12 document.

13 First, Your Honor, the Army
14 counter-intelligence report on WickiLeaks. Between the
15 ASIG website logs at Prosecution Exhibit 63 and summary
16 of the ASIG document, Special Agent Shaver, Prosecution
17 Exhibit 84, Pfc Manning viewed the ASIG report on at
18 five separate occasions starting from less than two
19 weeks after access on SIPRnet on 1 December '09 through
20 7 March 2010.

21 ASIG report is Prosecution Exhibit 45 and

1 46. (inaudible) testified the purpose of the ASig
2 document was to assess counter-intelligence threat to
3 the U.S. army posed by WikiLeaks.

4 As you look at Prosecution Exhibit 45, Your
5 Honor, please note, note that the first bullet point
6 under key judgment of ASig report is that WikiLeaks
7 represents a potential force protection,
8 counter-intelligence OPSEC and (inaudible) to United
9 States Army. Essentially the same language Pfc Manning
10 used when he taught the dangers of OPSEC violations.

11 The second bullet states, recent
12 unauthorized releases of DoD sensitive and classified
13 information documents provide foreign intelligence
14 services, foreign terrorists groups, insurgents and
15 other foreign adversaries potentially actionable
16 information targeting U.S. forces.

17 Your Honor, the sixth bullet states that
18 WikiLeaks most likely has other DoD sensitive and
19 classified information in its possession and will
20 continue to post the information on the website.

21 Finally, the report concluded that it must

1 be presumed that foreign adversaries will review and
2 assess any DoD sensitive or classified information
3 posted for the WikiLeaks website.

4 Pfc Manning sent reports to WikiLeaks with
5 the intent that they be released to the world. And it
6 was, Your Honor.

7 Your Honor, second the intelligence
8 information IRR, dated 23 March 2008 titled Internet
9 Web Posting of classified and official use only
10 documents. Prosecution Exhibit 99.

11 First, Your Honor, what is IRR? That's a
12 report used by intelligence professionals to report
13 analysis of raw intelligence. The purpose of this IRR
14 was to raise the awareness as a threat to national
15 security.

16 Special Agent Shaver that he created
17 Prosecution Exhibit 85. That was a summary of the
18 intel log information related to the IRR, and later I
19 will talk about, Your Honor, a C3 document.

20 THE COURT: What exhibit?

21 MAJOR FEIN: Exhibit 85. That summary

1 relates to and shows that Pfc Manning downloaded this
2 report on 14 February 2010. Found on Line 19 of that
3 exhibit.

4 The purpose of that IRR was to raise the
5 awareness of the threat caused by WikiLeaks to the
6 intelligence community. IRR discussed WikiLeaks is
7 publicly accessible website where the leaked
8 information includes classified and for official use
9 only, can be published to the public anonymously.

10 The report described the threat of
11 publishing classified information. It also detailed
12 the release of a Camp Delta SOP, GITMO, that was
13 unclassified, for official use only and caused concerns
14 within the United States Government.

15 Your Honor, Pfc Manning also compromised
16 this document to WikiLeaks. Line 5 of Prosecution
17 Exhibit 127. That's a volumes.txt data. That is when
18 a CD was burned on a SIPRnet computer, date and time of
19 that burn, the file name and folder structure. And
20 that was created on his personal MAC. Once you take a
21 CD, burn, put it into the MAC computer it creates a log

1 file.

2 That was Line 5, Your Honor. Third, the
3 report dated 7 January 2010, that I have already
4 referenced is a 3C report. This is the trip report
5 discussing the Marine Corp monitoring the chaos
6 communications Congress that was held 26 to 30 December
7 2009 in Germany.

8 This report, Your Honor, Prosecution
9 Exhibit 43. Your Honor, going back to Prosecution
10 Exhibit 85, the summary that Special Agent Shaver
11 created for the IRR, the 3C document. Line 12 shows
12 that Pfc Manning downloaded that document 14 February
13 2010 as well.

14 (Inaudible) the author of the document
15 testified that the document was posted to its unit
16 portal on SIPRnet and the address at Line 12 was the
17 address for that article.

18 Sergeant (inaudible) also testified that
19 the purpose of the report was to identify a potential
20 threat by WikiLeaks, particularly a security threat
21 that the owners may be venerable to. And then his

1 analysis was how to fix that vulnerability. The report
2 discussed that WikiLeaks publicly accessible internet
3 website, leaked information, including classified
4 information can be published.

5 On Page 3 of Prosecution Exhibit 43, the
6 report, analysis states WikiLeaks.org poses a large
7 threat not only from the external disclosure but also
8 from the insider. The insider within the Department of
9 Defense. The insider would be able to leak information
10 without fear of any direct individual repercussions.

11 Your Honor, Pfc Manning compromised this
12 document to WikiLeaks. That is clear by looking at
13 the file titled C3 on the .txt printout, Prosecution
14 Exhibit 127.

15 Your Honor, through his constant searches,
16 systematic review of intelligence reports, Pfc Manning
17 knew exactly what type of information he was providing
18 classified information to an organization that diverse
19 elements of the U.S. military reported was a threat to
20 the national security interest of United States
21 Government.

1 Your Honor, in addition to the research
2 that he conducted, also looked at Pfc Manning's actual
3 thoughts on WikiLeaks, as captured in his chat logs
4 with Lamo and Julian Assange.

5 These chat logs confirm that Pfc Manning
6 saw WikiLeaks as anything but a journalistic
7 enterprise. Pfc Manning saw WikiLeaks as an
8 intelligence agency. And that Pfc Manning knew that
9 WikiLeaks' goals in the methods were different than
10 anything that could be characterized as traditional
11 journalism.

12 Your Honor only needs to look as far as the
13 chats to Julian Assange, Prosecution Exhibit 123. That
14 is the Assange chats. Page 9, Your Honor. Pfc Manning
15 identified WikiLeaks as the first intelligence agency
16 for the general public. And in his own words, because
17 it did everything an intelligence agency does, minus
18 the anonymous sourcing.

19 Page 10 of the chats, Your Honor. Julian
20 Assange confirmed this evaluation and noted that the
21 original WikiLeaks described WikiLeaks as the first

1 intelligence agency of the people, better principled
2 and less parochial than any Government intelligence
3 agency. Its only interest in revelation of the truth.

4 Even when discussing the substantive of the
5 information that he compromised Pfc Manning
6 acknowledged what was in the documents would make it
7 look more like journalist acquired it. That's on Page
8 2.

9 And what did Julian Assange say about his
10 operation to Pfc Manning? He talked about giving an
11 Intel source a list of things he wanted. Page 7. He
12 talked about outing another spy this afternoon. Page
13 11.

14 He asked Pfc Manning if there's some way I
15 can get you a crypto phone. Page 11. Crypto phone,
16 secure communications with Pfc Manning in Southeast
17 Baghdad.

18 Pfc Manning knew anything he disclosed
19 WikiLeaks would be published on the internet for the
20 world to see. It is clear Pfc Manning wanted this
21 information to be in the public domain.

1 The Asig report, which Pfc Manning
2 repeatedly read and compromised discusses the DoD
3 classified information that WickiLeaks released in the
4 past and how WickiLeaks posts all information they
5 receive without editorial oversight.

6 The Asig report also says that WickiLeaks
7 aimed for maximum political impact. The C3 document
8 stated that the goal of WickiLeaks was to create
9 openness. And Prosecution Exhibit 30, these are the
10 chats, Lamo chats, Your Honor, Pfc Manning admitted
11 that he trained his documents to WickiLeaks he couldn't
12 let these things stay inside the system and inside of
13 his head. Page 26.

14 He also specifically admitted that the
15 information he sent to WickiLeaks, belongs to the board
16 of public domain, the information should be free. Page
17 40. He also stated about the Apache video. Event
18 occurring 2007, I watched video in 2009 with no context
19 to research, forward information to a group of Freedom
20 of Information Act. Page 33.

21 Your Honor, the chats with Assange Pfc

1 Manning says, I told you before Government
2 organizations can't control information. The harder
3 they try the more violently the information wants to
4 get out. That's Page 5, Your Honor.

5 When discussing WikiLeaks obtaining
6 information from a public figure's email account and
7 posting that information, Pfc Manning says, well, I
8 don't know what a posting of a list of (inaudible) but,
9 hey, its transparency. Page 5.

10 Your Honor, setting aside semi-classified
11 documents to established journalistic enterprise like
12 New York Times or Washington Post would be a crime.
13 That is not what happened in this case under these
14 facts.

15 Pfc Manning deliberately and intentionally
16 disclosed his compromised information through
17 WikiLeaks to the world knowing that WikiLeaks would
18 release the information in the form they received it
19 and that is, Your Honor, that is exactly what happened
20 in this case.

21 WikiLeaks was merely the platform which

1 Pfc Manning used to ensure all the information was
2 available for the world, including the enemies of the
3 United States.

4 Your Honor, Defense offered Professor
5 Benkler as an expert in the network for (inaudible).
6 Professor Benkler's is based on bias, misinformation
7 and a flawed methodology. It provides no utilities
8 because regardless of his conclusions, Your Honor,
9 Professor Benkler can give you no insight in what Pfc
10 Manning was thinking at the time he was deployed.

11 Professor Benkler based his opinions
12 largely on a review of articles, news articles, post
13 July 2010, several months after Pfc Manning was placed
14 in pretrial confinement.

15 However, if there's any utility to
16 Professor Benkler's testimony it was in his answers to
17 several questions posed to him on journalistic
18 enterprises, in general questions that used Pfc Manning
19 own word.

20 Professor Benkler agreed that a
21 transparency movement is not a journalistic enterprise.

1 He agreed that information activist is not a
2 journalistic enterprise. He agreed there's a
3 difference between activism and journalism.

4 WickiLeaks, an organization with a mission
5 for transparency of U.S. Government classified
6 information for the purpose of maximizing political
7 impact. Information -- well, essentially, Your, Honor
8 information anarchist. That failed to meet even
9 Professor Benkler's criteria for a journalistic
10 enterprise.

11 Your Honor, Professor Benkler testified
12 that his main sources of information were the news
13 articles he reviewed, which he then assigned values to
14 in some way that's not entirely transparent. And used
15 some critiques he received from Julian Assange when he
16 posted his draft article on his personal web page.

17 Professor Benkler conducted no independent
18 research on any aspect of WickiLeaks, including the
19 ASig reports, or WickiLeaks, nor did he interview
20 anyone with firsthand knowledge of WickiLeaks.

21 He clearly had a point of view and strong

1 opinions. But Professor Benkler did not have access to
2 the evidence in this case revealing what Pfc Manning
3 actually knew and thought of the WikiLeaks
4 organization, nor did he have access to the evidence
5 that demonstrated how WikiLeaks actually operated
6 outside the news report he analyzed and researched.

7 Reporting that any knowledge was very poor
8 at the time. As an example of professor Benkler's
9 faulty process he concluded that WikiLeaks acted
10 responsibly by characteristic of a traditional news
11 media, hand selected or redacted December cables in
12 2010.

13 He spent much time testifying that
14 80 percent incorrectly reported that WikiLeaks
15 released over 250,000 Department of State cables onto
16 the internet at that time, when he counted only 272
17 cables based on other news reports, correlating news
18 reports.

19 He further concluded that WikiLeaks
20 continued to follow that model in all of their
21 releases. Had Professor Benkler actually conducted

1 independent research outside of news reports, such as
2 contacting WikiLeaks, editors of newspapers, or any
3 other person with firsthand knowledge, he would have
4 quickly realized that WikiLeaks actually did release
5 251,287 purported cables on the internet in unredacted
6 form, as well as other databases of information that
7 Pfc Manning compromised.

8 Your Honor, regardless of what Professor
9 Benkler, the defense of United States believes
10 WikiLeaks is or is not, the evidence is clear that Pfc
11 Manning believed the organization to be his conduit to
12 release as much information as he could obtain.

13 But why did he choose WikiLeaks? He chose
14 WikiLeaks because they sought, almost exclusively,
15 from the United States, United States Government
16 classified information, and that is what Pfc Manning
17 could provide them as an intelligence analyst on
18 SIPRnet.

19 The three intelligence reports, all said
20 that WikiLeaks, any type of classified information as
21 well as PII and their operational data. In chats with

1 Julian Assange Pfc Manning showed his understanding
2 that WikiLeaks was seeking to publish Government
3 controlled information, said to them by him and other
4 donors.

5 Your Honor, that shows that WikiLeaks
6 produced a Most Wanted List available on its website.
7 That it identified to the reader the type of
8 information that they sought, to gather and disclose in
9 the name of transparency information anarchy. Looking
10 at both versions of the Most Wanted List, Prosecution
11 Exhibit 109 or 110 and the Defense unsorted list,
12 Defense Exhibit Foxtrot or Defense Exhibit Papa.

13 The largest section on the Most Wanted List
14 by several orders of magnitude, Your Honor, was the
15 section devoted to the United States, specifically the
16 section devoted to military intelligence documents on
17 Prosecution Exhibits 109 and 10 in bulk databases on
18 Defense Exhibits Foxtrot and Papa.

19 Less than two weeks after Pfc Manning had
20 regular access to SIPRnet, Pfc Manning began using
21 Intelink to search for items on that Most Wanted List.

1 (Inaudible) Prosecution Exhibit 81, you'll see the
2 searches on 28 November, 29, 30 November and 8 December
3 '09, that correspond with items on the Most Wanted
4 List. None of these have any relationship to a United
5 States Army Intelligence Analyst assigned to Southeast
6 Baghdad focused on a (inaudible)

7 Specifically, Your Honor, by 28
8 November 2009, Thanksgiving, Pfc Manning was searching
9 for information related to GITMO and interrogations.
10 Prosecution Exhibit 81 is a summary of those.

11 The Most Wanted List in 2009 shows that
12 WikiLeaks wanted CIA interrogation videos. Pfc
13 Manning searched for retention of interrogation videos.
14 The term retention of interrogation videos on 28 and 29
15 November 2009. That is Line 28 through 32 of PE 81.

16 Pfc Manning continued searching for
17 detainee videos on 9 December. Retention of
18 interrogation videos on Lines 28 through 32 of PE81.

19 Your Honor, Pfc Manning continued searching
20 for detainee videos on 9 December. That's Line 115
21 through 116. He conducted more searches for

1 interrogation videos on 17 December. Line 154 through
2 155. He conducted another search a month later at
3 Line 283.

4 Your Honor, the Most Wanted List of 2009
5 also shows that WikiLeaks wanted a detainee abuse
6 photos. Their term. Pfc Manning searched for the term
7 detainee abuse on 29 and 30 November, 2009. Lines 44
8 through 46. Line 63.

9 The Most Wanted List showed that WikiLeaks
10 wanted Camp Delta, Guantanamo standard operating
11 procedures. And Camp Delta, Guantanamo interrogation
12 standard operating procedures, 2003 through 2009.

13 Your Honor, Pfc Manning searched for
14 Guantanamo detainee operations, JTF, GITMO SOP and SOP
15 interrogation, among others, on 8 December. This is at
16 Line 101 through 112.

17 Pfc Manning continued the searched
18 throughout his deployment. 15 March Pfc Manning
19 searched Intelink for information on GITMO, ISN and
20 search. That was on Line 470 through 474.

21 Your Honor, Pfc Manning spent hours, hours

1 in late November 2009, early in December 2009,
2 searching for topics that only related to one mission,
3 finding and disclosing what WikiLeaks wanted.

4 He was not a naive soldier simply affected
5 by an event on 24 December 2009, an event that only
6 Chief Ehresman vaguely remembers, not even the exact
7 date, but rather Pfc Manning was deliberately taking
8 advantage of the trust and access to classified systems
9 in pursuit of his own objectives.

10 Think back to one of the first things that
11 Pfc Manning said to Lamo in the chats. If you had
12 unprecedented access to classified networks, what would
13 you do?

14 Pfc Manning answered that question with his
15 actions. He searched for as much information that he
16 knew would guarantee his fame, information that
17 WikiLeaks wanted to publicly release.

18 Your Honor, although he kept searching for
19 information on WikiLeaks Most Wanted List, Pfc Manning
20 also wanted to ensure he would not get caught.

21 So why did Pfc Manning chose to disclose

1 classified information through WikiLeaks and not
2 solely by himself for the world to have? He did not
3 want to get caught, Your Honor. Pfc Manning
4 anticipated needing to slip into the darkness for a few
5 years, let the heat die down. At least that's what he
6 Julian Assange on the chats on Page 5.

7 Prosecution Exhibit 42. He instructed
8 WikiLeaks to protect their source, protect him. The
9 ASig report on the IRR, informed Pfc Manning as early
10 as December '09 that WikiLeaks used anonymous methods
11 to post information online.

12 The ASig report detailed that WikiLeaks
13 uses its own software which can make it difficult for
14 foreign governments and foreign business to determine
15 where the leak document was and who is responsible for
16 leaking that document.

17 Your Honor, the IRR described WikiLeaks as
18 an un censorable Wikipedia for untraceable mass
19 document leaking analysis. The IRR included that the
20 WikiLeaks website provides suggestions for the
21 anonymous submission of material and several methods of

1 submitting material for inclusion to an online
2 database.

3 Your Honor, right now might be a good time
4 for a brief recess before I get going.

5 THE COURT: All right. How much longer do
6 you anticipate your argument is going to be? I'm
7 looking at whether we should recess for lunch.

8 MAJOR FEIN: I can probably get through one
9 more section and then recess for lunch. Overall I
10 anticipate two more full hours.

11 THE COURT: Why don't we take a 15 minute
12 recess, get through the next session and take a lunch
13 break.

14 MR. COOMBS: I would like to know maybe how
15 long the section is. If the next session is an hour, I
16 would rather break for lunch now.

17 MAJOR FEIN: It's not. Actually, I can
18 probably get to the next session, right now it is the
19 first set of data that was compromised. Probably last
20 15 minutes. The section after that is lengthy, Your
21 Honor, after the next section.

1 THE COURT: All right. Mr. Coombs, do you
2 have any grave objection here to taking a quick 15
3 minute recess, finishing up with that 15 minutes and
4 then taking a lunch break after that?

5 MR. COOMBS: No, objection, Your Honor.

6 THE COURT: The court will recess until
7 five after 12:00.

8 (Recess)

9 THE COURT: Court is called to order.
10 Record show that all parties present when the Court
11 last recessed are present in Court. Major Fein.

12 MAJOR FEIN: Yes, ma'am. The first dataset
13 is (inaudible). This case starts with Pfc Manning's
14 admission to Mr. Lamo that he had helped WickiLeaks
15 right Thanksgiving 2000.

16 How did Pfc Manning begin helping
17 WickiLeaks? By transmitting the video file charged in
18 Specification 11, Charge 2.

19 Specification 11 in Charge 2. Your Honor,
20 what we know about the Garani air strike video and why
21 is it important? Pfc Manning admitted to Adrian Lamo

1 that he gave it to WikiLeaks. Lamo chat logs, Page
2 46. Jason Katz, an employee of Brocadia National labs
3 had a copy on his computer dated 15 December 2009.

4 We know that the video was encrypted
5 (inaudible). We know that WikiLeaks tweeted on 8
6 January 2010, that they needed assistance with
7 decrypting a video. These are undisputed facts.

8 So why, Your Honor, is the Defense fighting
9 so hard to disprove this timing. Because the evidence
10 destroys, Your Honor, their narrative that Pfc Manning
11 witnessed an event that helps explain his actions
12 rather than accepting the facts as they -- Pfc Manning
13 was only interested in disclosing classified
14 information to the world through WikiLeaks.

15 We start within weeks of having access to
16 SIPRnet. And he chose a video that he could not even
17 watch, a password protected video.

18 Pfc Manning accessed this video before 1
19 December 2009 (inaudible). He transferred the video to
20 his personal Mac and uploaded to WikiLeaks before 15
21 December 2009. So that lands in the hands of a person

1 willing to assist WikiLeaks with a mass decryption
2 effort.

3 THE COURT: Can you speak a little more
4 slowly?

5 MAJOR FEIN: Yes, Ma'am. Pfc Manning
6 accessed this video before 1 December 2009. That was
7 on the (inaudible) server. He transferred the video to
8 his personal Mac and uploaded it to WikiLeaks before
9 15 December 2009.

10 He did that, Your Honor, so it could land
11 in the hands, to assist in the decryption effort.

12 Your Honor, how do we know this? Special
13 Agent Shaver testified that DE22PAX.zip, that file name
14 contained in the video file within zip file called
15 BE22PAX.WMD. WMD is the Windows file, Windows movie
16 video type.

17 That video was located in the U.S.
18 (inaudible) site with documents that were part of the
19 (inaudible) investigation.

20 According to multiple U.S. CentCom subject
21 matter experts the investigation was focused on

1 investigating the circumstances surrounding a civilian
2 casualty (inaudible) incident.

3 Your Honor, Prosecution Exhibit 65 did the
4 (inaudible). In that exhibit, you'll see the file
5 BE22PAX.zip, which is also listed on the charge sheet,
6 is under the folder called videos.

7 Multiple CentCom witnesses testified video
8 operational activities, including troop movement,
9 weapon systems and specific information contained on
10 the heads up display.

11 In classified testimony, through a
12 stipulation of expected testimony that the video
13 reveals other details of military preparedness.

14 Your Honor, what we know forensically about
15 Pfc Manning in the late November 2009 and early
16 December 2009 time period, Your Honor, between 29
17 November 2009 and 9 December 2009, Pfc Manning searched
18 several times on SIPR intelling specifically for the
19 terms SJA and CentCom. That's in Prosecution Exhibit
20 81.

21 Those searches would have brought Private

1 First Class Manning to the U.S. SJA website, the legal
2 website, Intel only shows searches and redirects, as
3 you heard Special Agent Shaver, to other websites.
4 They don't actually account for activity. It's on a
5 separate server. The CentCom SharePoint server was a
6 separate server.

7 Mr. Moiser, senior paralegal for the U.S.
8 CentCom SJA office and the administrator of the U.S.
9 Share Point page, he testified the (inaudible) videos
10 located on Share Point server.

11 Your Honor Prosecution Exhibit 91 is a copy
12 of the portal web page. Five screen shots of that
13 page, Your Honor. Note, Your Honor, when you review
14 Prosecution Exhibit 91, across the top each of the web
15 pages is a red banner. And that red banner has
16 "secret" approximately five times spread across the top
17 of that page.

18 Prosecution Exhibit 91 screen shots all the
19 different folders within the SJA investigations share
20 the (inaudible) that leads to videos BE22PAX.zip. Your
21 Honor, that banner put any visitor, including Pfc

1 Manning, on notice that the information on that website
2 should at least be treated classified.

3 Special Agent Shaver (inaudible) duplicate,
4 Your Honor, of that on Jason Katz's computer. Although
5 the file he found was named B.zip. Jason Katz, an
6 employer of the laboratory created B.zip on 15
7 December 2009. Had his computer plug into the lab's
8 super computer, which is capable of breaking into or
9 decrypting files.

10 Your Honor, Prosecution Exhibit 32 is a
11 tweet from WikiLeaks on 8 January 2010, which states,
12 having crypt-ed videos of U.S. bomb strikes on
13 civilians with a web page, says Afghan, we need super
14 computer time. That was on 8 January 2010.

15 Your Honor, this WikiLeaks tweet, the
16 encrypted file on Katz's computer, which is connected
17 to the super computer, and Pfc Manning's admissions,
18 all lead to one conclusion. The transmission of the
19 video occurred prior to 15 December 2009. And based on
20 the evidence available to the Court, there's no other
21 reasonable explanation.

1 And here's why, Your Honor. First Special
2 Agent Shaver, Mr. Johnson, the other forensic examiner,
3 testified they did not find any remnants or evidence of
4 the videos running videos on any of the computers they
5 examined.

6 We know that nothing was recoverable by the
7 personal act before the 31 January 2010 or SIPRnet
8 computers from March 2010, because they were reimaged.
9 Personal Mac, because he forensically wiped his
10 computer using a 7 pass forensic wipe. Pfc Manning did
11 that.

12 Second, Your Honor, Special Agent Shaver
13 testified that when he reviewed the U.S. CentCom share
14 Point server logs, so the actual server logs that
15 housed the videos, that's Prosecution Exhibit 108. The
16 log started on 1 December 2009. They captured all the
17 access activity of the files in the folder that sat on
18 the CentCom website.

19 Those logs, Your Honor, 1 December 2009.
20 After that date the logs showed that the video was only
21 accessed twice. Once on 28 January 2010 and again on

1 23 February 2010.

2 Now first, Your Honor, Pfc Manning could
3 not have accessed the video on that date because he was
4 in Boston on R&R leave. Pfc Manning did not access the
5 video on 23 February 2010. The reason we know that is
6 because of the Sintar logs. That captured threat data
7 for this case between Pfc Manning's SIPRnet computers
8 and other destinations do not show any connections to
9 the CentCom Share Point server on 23 February 2010.

10 Now, Your Honor, note at Prosecution
11 Exhibit 161, Special Agent Shaver testified that he
12 created this summary, Prosecution Exhibit 161, that
13 shows all the missing dates from the Sintar logs. So
14 his testimony was the Sintar logs were complete, but he
15 testified that certain days he knew were complete
16 because there were some activity that showed and other
17 days it was completely void.

18 At line 58 of Prosecution Exhibit 161
19 showed that 23 February 2010, was reported within
20 Sintar and not missing from the logs. And there was no
21 entry from the a logs, as Special Agent Shaver

1 testified, between Pfc Manning's SIPRnet computer and
2 the port on 23 February 2010.

3 Third, at trial the Defense referenced the
4 video file titled (inaudible). You heard testimony
5 that it was located in a folder named (inaudible), a
6 shared drive at FOB Hammer.

7 This file, Your Honor, on a Microsoft
8 Windows computer, keeps track of the last ten times a
9 file type is opened. WMV.

10 Special Agent Shaver testified that
11 (inaudible) was listed in the NT user file under the
12 WMV file type on Pfc Manning's SIPRnet computer. Your
13 Honor, this means that Pfc Manning opened (inaudible)
14 on his SIPRnet computer.

15 The issue here is that it could not be
16 BEPAX22.WMV because that video, the charge video was an
17 encrypted zip file. Thus, unable to be opened and
18 viewed by Pfc Manning. And could not show up in the NT
19 user file as a WMV viewed file.

20 Your Honor, fourth, Prosecution Exhibit 128
21 is the summary of all the (inaudible) related activity

1 in the index.dac file on Pfc Manning's SIPRnet
2 computer. That's Prosecution Exhibit 128.

3 Special Agent Shaver testified in the
4 index.dac records, that file records the dates and
5 times the files are accessed either locally or remotely
6 through a web browser for Windows.

7 Also testified on 10 April 2010, the day
8 Pfc Manning downloaded the entire investigation, less
9 the videos, from the Share Point site, there was no
10 video file or zip file reflected in the activity on his
11 SIPRnet computer. All the other files were downloaded
12 but not a zip file or WMV file.

13 Your Honor, look at Prosecution Exhibit
14 129. That is the summary of the logs on 10 April 2010.
15 Index.dac, Prosecution Exhibit 128, shows activity Pfc
16 Manning's computer connecting to Share Point logs and
17 Exhibit 129 next in line, a summary of the actual share
18 Point logs from the CentCom website. Activity on 10
19 April 2010.

20 The CentCom logs show the other side of the
21 download transaction. The CentCom site. Every

1 document downloaded from the CentCom Share Point site
2 on 10 April 10 that is associated with Farrah is
3 located in that summary.

4 Most importantly, Your Honor, there is no
5 video CentCom downloaded during that time on those logs
6 also.

7 Your Honor, the video must have been
8 downloaded prior to 1 December 2009 and transmitted no
9 later than 15 December 2009. Your Honor, Pfc Manning
10 knew his video along with the other videos were
11 classified.

12 Although the file name did not have
13 annotation, the file was located on SIPRnet with a
14 secret banner across the top of his scene. The video
15 relates to the national defense of the United States,
16 which the video contained the type of information which
17 could cause serious harm to national security and thus
18 should be secret.

19 (Inaudible) U.S. CentCom Deputy Commander
20 duly appointed original classification authority
21 testified that the charge video was properly classified

1 at the secret level. And, Your Honor, the United
2 States Government has never made this video available
3 to the public as part of a 15-6 or any other.

4 Now at this time would be a good time for
5 lunch recess.

6 THE COURT: All right. We come back at
7 1330. Does that work for everybody?

8 MR. COOMBS: Yes, ma'am.

9 THE COURT: Court is in recess until 1330.

10

11

12

13

14

15

16

17

18

19

20

21

<p>A</p> <p>abide (1) 24:4</p> <p>ability (2) 5:19;14:21</p> <p>able (2) 38:2;55:9</p> <p>absent (2) 4:6,19</p> <p>abuse (2) 66:5,7</p> <p>abused (2) 8:13;27:18</p> <p>Abusing (1) 10:4</p> <p>accepted (2) 26:15,16</p> <p>accepting (1) 71:12</p> <p>access (26) 10:4,15;11:13;16:8,19; 17:10;21:16;25:1,9;27:1,17, 18;36:17;46:15,16;47:1; 48:17;50:19;62:1,4;64:20; 67:8,12;71:15;76:17;77:4</p> <p>accessed (6) 16:10;71:18;72:6;76:21; 77:3;79:5</p> <p>accessible (4) 29:4;38:17;53:7;55:2</p> <p>accomplish (2) 17:11;40:17</p> <p>accomplished (1) 44:4</p> <p>accordance (1) 5:21</p> <p>according (6) 20:9;30:1;32:7;46:13; 47:15;72:20</p> <p>account (6) 4:3;49:1,6,16;59:6;74:4</p> <p>accountable (2) 33:4,9</p> <p>accounting (1) 5:7</p> <p>accrue (1) 8:9</p> <p>acknowledged (1) 57:6</p> <p>acknowledgments (2) 10:7;25:8</p> <p>acquired (1) 57:7</p> <p>across (5) 16:5,14;74:14,16;80:14</p> <p>Act (2) 58:20;76:7</p> <p>acted (1) 62:9</p> <p>action (2) 9:20;27:13</p>	<p>actionable (2) 45:7;51:15</p> <p>actions (3) 40:21;67:15;71:11</p> <p>actively (1) 49:15</p> <p>activism (1) 61:3</p> <p>activist (1) 61:1</p> <p>activists (1) 35:8</p> <p>activities (4) 20:15,20;30:3;73:8</p> <p>Activity (15) 9:14;16:5,12;39:13; 41:13;42:10;43:9,9;74:4; 76:17;77:16;78:21;79:10, 15,18</p> <p>acts (2) 10:14;33:5</p> <p>actual (7) 12:13;18:3;29:13;32:19; 56:2;76:14;79:17</p> <p>actually (14) 6:13;7:8;9:2;10:11; 12:15;30:14,20;48:16;62:3, 5,21;63:4;69:17;74:4</p> <p>addition (3) 23:16;29:18;56:1</p> <p>additional (2) 5:1;29:11</p> <p>Additionally (1) 4:7</p> <p>address (4) 7:11;16:18;54:16,17</p> <p>addresses (1) 34:17</p> <p>administrator (1) 74:8</p> <p>admission (1) 70:14</p> <p>admissions (1) 75:17</p> <p>admitted (5) 13:13;23:17;58:10,14; 70:21</p> <p>Adrian (2) 15:2;70:21</p> <p>advanced (1) 6:14</p> <p>advantage (1) 67:8</p> <p>adversaries (6) 26:9;35:5,10;36:9;51:15; 52:1</p> <p>adversary (1) 21:2</p> <p>advise (1) 7:5</p> <p>affected (1) 67:4</p> <p>Afghan (1)</p>	<p>75:13</p> <p>Afghanistan (1) 15:17</p> <p>afternoon (1) 57:12</p> <p>again (8) 4:5;5:14;6:10,21;7:20; 32:8,10;76:21</p> <p>against (6) 22:1,1,21;33:1;42:20; 45:11</p> <p>agency (8) 11:4,6;49:9;56:8,15,17; 57:1,3</p> <p>Agent (14) 20:1;49:12;50:16;52:16; 54:10;72:13;74:3;75:3; 76:2,12;77:11,21;78:10; 79:3</p> <p>Agnet (1) 47:4</p> <p>agreed (3) 60:20;61:1,2</p> <p>agreement (4) 25:5;26:16,21;27:4</p> <p>agreements (5) 25:7,18;27:10,12,15</p> <p>aided (1) 13:8</p> <p>aimed (1) 58:7</p> <p>air (1) 70:20</p> <p>Airborne (1) 46:19</p> <p>airstrike (1) 15:21</p> <p>AIT (9) 17:14,15,19;21:13;22:18; 24:19;27:20;29:18;32:14</p> <p>allegiance (1) 8:4</p> <p>Allen (1) 49:7</p> <p>allowed (2) 18:14;19:8</p> <p>allows (2) 40:5;41:9</p> <p>almost (1) 63:14</p> <p>along (2) 34:7;80:10</p> <p>al-Qaida (7) 13:10,10;22:17;23:8,10; 29:16,17</p> <p>alternate (1) 4:13</p> <p>Although (6) 13:18;44:14;45:5;67:18; 75:4;80:12</p> <p>Always (1) 21:1</p> <p>Ambassador (1)</p>	<p>48:5</p> <p>among (2) 39:17;66:15</p> <p>amount (2) 28:1;42:12</p> <p>amounts (2) 11:16;16:12</p> <p>ample (1) 47:9</p> <p>analyses (1) 30:11</p> <p>analysis (22) 31:19;40:12,13;42:4; 43:4,5,5,6,8,10,11,14,21; 44:1,15;45:6,9;50:2;52:13; 55:1,6;68:19</p> <p>analyst (25) 8:11;12:8;17:10,12;21:5; 24:18;29:21;30:20;36:5,11; 37:18,18;38:5,11,19;39:3; 43:1,17;44:9,10;45:3,5; 48:10;63:17;65:5</p> <p>analysts (20) 30:11;32:3;38:12,14,17; 39:8,11,12,19;40:3,5,9,18; 41:16;44:4,12,14,18,21; 45:7</p> <p>analyze (2) 41:3,5</p> <p>analyzed (1) 62:6</p> <p>anarchist (1) 61:8</p> <p>anarchy (2) 9:6;64:9</p> <p>anguished (1) 9:18</p> <p>Anika (2) 31:9,15</p> <p>annotation (1) 80:13</p> <p>anonymous (3) 56:18;68:10,21</p> <p>anonymously (2) 11:15;53:9</p> <p>answered (1) 67:14</p> <p>anticipate (2) 69:6,10</p> <p>anticipated (1) 68:4</p> <p>Anti-Terrorism (1) 28:16</p> <p>Apache (3) 20:2,7;58:17</p> <p>apparent (1) 45:15</p> <p>Appellate (4) 5:2,9,11;6:2</p> <p>Appendix (1) 29:6</p> <p>Apple (1) 14:12</p>
---	--	--	--

applicable (1) 42:6	assesses (1) 45:4	Balonek (3) 27:6;30:14,16	75:12
appointed (1) 80:20	assessment (2) 31:18;43:2	banner (4) 74:15,15,21;80:14	borne (1) 31:18
appreciated (1) 12:9	assessments (1) 31:19	based (9) 24:2;40:21;43:9,19;44:6; 60:6,11;62:17;75:19	Boston (1) 77:4
approximately (3) 32:8;47:17;74:16	assets (2) 34:3,4	basis (2) 37:12;42:16	both (5) 24:14;27:14;43:21;50:3; 64:10
April (7) 16:13;26:2;47:8;79:7,14, 19;80:2	assigned (8) 32:10;36:11;38:14,20; 40:10;44:5;61:13;65:5	battalion (1) 40:7	bottom (2) 18:21;21:2
Arabian (2) 13:11;29:17	assist (4) 17:2;45:6;72:1,11	battlefield (1) 34:8	box (1) 4:10
area (2) 31:19;32:6	assistance (2) 32:5;71:6	BE22PAXWMD (1) 72:15	Bradley (2) 8:3;33:20
areas (2) 30:3;43:15	assisting (1) 11:12	BE22PAXzip (2) 73:5;74:20	BradS87 (1) 49:2
argues (1) 14:3	associated (1) 80:2	began (5) 45:15;46:1,16;49:6;64:20	break (4) 7:14;69:13,16;70:4
argument (8) 5:13;6:15;7:6,7,8,12; 12:1;69:6	assume (1) 21:1	begin (1) 70:16	breaking (1) 75:8
arise (1) 7:2	assurance (2) 23:18;24:14	beginning (2) 46:21;47:6	brief (6) 7:13,17;28:9;31:12; 42:15;69:4
arm (1) 42:20	attack (2) 9:7;22:14	behavior (1) 43:8	briefed (2) 26:2,5
armed (3) 8:7,8;13:6	attacks (2) 30:5;42:13	believes (1) 63:9	briefing (5) 15:13;18:1;19:17;34:10; 35:17
arms (1) 30:7	attempt (1) 20:13	belongs (1) 58:15	briefly (1) 6:18
army (18) 15:12;18:4,12;26:3; 27:21;28:11,15,20;29:5; 35:3;38:19;40:20;41:8; 48:10;50:13;51:3,9;65:5	attended (1) 17:15	benefit (1) 43:18	brigade (5) 31:13;36:13,19;42:20; 46:19
Army's (1) 34:8	audience (1) 20:21	benefits (1) 43:18	bright (1) 20:19
arrived (2) 32:13,15	audit (1) 16:3	Benkler (9) 60:5,9,11,20;61:11,17; 62:1,21;63:9	Brocadia (1) 71:2
arriving (2) 8:12;46:3	author (1) 54:14	Benkler's (4) 60:6,16;61:9;62:8	Brook (1) 15:19
art (1) 43:8	authorities (2) 18:13;19:7	BEPAX22WMV (1) 78:16	brought (4) 15:6,11;33:3;73:21
article (2) 54:17;61:16	authority (1) 80:20	best (2) 9:7;11:20	browser (1) 79:6
articles (3) 60:12,12;61:13	authorized (2) 21:9,10	better (1) 57:1	Buchanon (1) 39:14
aside (1) 59:10	available (8) 4:14;17:6;29:1;49:18; 60:2;64:6;75:20;81:2	bias (1) 60:6	building (1) 36:13
Asig (12) 50:11,15,16,17,21;51:1,6; 58:1,6;61:19;68:9,12	avoid (1) 35:18	bigger (1) 10:5	bulk (1) 64:17
aspect (1) 61:18	aware (1) 10:19	bin (1) 23:8	bullet (3) 51:5,11,17
Assange (21) 11:3;15:2;17:2;45:19,20; 46:9;47:9;48:7,12;49:17,19, 20;56:4,13,14,20;57:9; 58:21;61:15;64:1;68:6	awareness (2) 52:14;53:5	birth (1) 34:17	burn (2) 53:19,21
Assange's (1) 14:16		black (1) 26:9	burned (3) 15:5;20:6;53:18
assess (3) 45:3;51:2;52:2		blog (1) 20:21	business (1) 68:14
	back (4) 48:11;54:9;67:10;81:6	blue (1) 18:20	Bzip (2) 75:5,6
	background (1) 39:21	board (1) 58:15	
	bad (1) 31:12	bold (1) 20:19	
	Baghdad (4) 40:14;48:10;57:17;65:6	bomb (1)	
			C
			C3 (4)

50:11;52:19;55:13;58:7 cable (2) 48:2,3 cables (4) 62:11,15,17;63:5 calculating (1) 10:13 called (7) 4:2;7:18;21:3,16;70:9; 72:14;73:6 came (2) 6:19;32:3 Camp (3) 53:12;66:10,11 can (17) 5:21;18:8;21:17;22:14, 21;24:10;25:18;41:5;47:11; 53:9;55:4;57:15;60:9; 68:13;69:8,17;72:3 capabilities (7) 23:4;29:1;34:8;35:2; 39:6;44:16;45:9 capability (1) 44:11 capable (3) 29:7;44:11;75:8 capacity (1) 4:15 Captain (7) 4:6,6;37:9;42:3,7,11;44:3 captured (4) 16:4;56:3;76:16;77:6 card (2) 9:15;15:15 cared (1) 9:3 carelessness (1) 9:3 case (9) 11:17;13:12;15:8;20:1; 59:13;20;62:2;70:13;77:7 cases (1) 7:2 casualty (1) 73:2 cataloged (1) 28:3 caught (2) 67:20;68:3 cause (3) 18:8;28:18;80:17 caused (3) 13:3;53:5,13 CD (3) 20:5;53:18,21 CDs (2) 15:5,6 cell (2) 32:10;40:11 cells (1) 32:5 censorable (1) 68:18	CentCom (14) 72:20;73:7,19;74:5,8; 76:13,18;77:9;79:18,20,21; 80:1,5,19 Center (6) 4:9;49:1,8,16,18;50:2 Central (1) 49:9 certain (6) 15:1,4;32:6;39:21;41:13; 77:15 certificates (1) 23:18 changed (1) 4:19 chaos (1) 54:5 chapel (1) 4:14 characteristic (1) 62:10 characterized (1) 56:10 Charge (7) 5:5;31:7;70:18,19;73:5; 78:16;80:21 charged (1) 70:17 charges (1) 13:21 chat (4) 48:7;56:3,5;71:1 chatrooms (1) 35:14 chats (15) 9:4;11:6;15:1;46:5;49:3, 20;56:13,14,19;58:10,10, 21;63:21;67:11;68:6 Chavez (1) 4:19 Chief (8) 27:6;30:14,16;42:3,17; 43:1,12;67:6 choose (1) 63:13 chooses (1) 21:10 chose (4) 12:10;63:13;67:21;71:16 chronological (1) 12:18 CIA (1) 65:12 CIDNE (2) 31:17;39:8 CIDNI (1) 15:16 circumstances (1) 73:1 civilian (1) 73:1 civilians (1) 75:13	Class (9) 13:19;17:15;20:10;21:15; 30:2;31:9;47:21;48:4;74:1 classification (5) 18:5;21:9;25:14,17;80:20 classified (55) 5:12;8:9,15;9:16;10:15; 11:9,13;16:5;18:16,17,17; 19:1,5,12,14,16;20:8;25:1, 9,12;26:3,10;27:1,5,11,17, 19;33:6;36:14;37:2,6,11,13, 19;50:9;51:12,19;52:2,9; 53:8,11;55:3,18;58:3;61:5; 63:16,20;67:8,12;68:1; 71:13;73:11;75:2;80:11,21 classify (1) 18:13 classifying (1) 18:11 clear (6) 10:16;11:18;32:12;55:12; 57:20;63:10 clearance (6) 24:19,19;25:3;26:8; 36:17,21 clearly (1) 61:21 Clinton (1) 9:6 closely (8) 10:7;14:8,13,15;29:14; 35:6,12;36:7 closing (3) 5:13;6:15;7:12 cognizant (1) 11:17 coldly (1) 48:6 collaboration (2) 39:17;40:4 collate (2) 40:20;41:2 Colonel (4) 31:14;36:19;37:14;42:15 combat (1) 10:3 combined (3) 22:8;32:18,19 command (1) 42:16 commander (5) 31:14;36:19;44:1,20; 80:19 commit (1) 38:2 committed (2) 13:19;27:16 common (2) 35:11,21 commonly (2) 39:7,10 communicate (1) 14:15	communications (2) 54:6;57:16 community (4) 11:10;14:9;39:18;53:6 compiled (1) 30:19 complete (3) 38:20;77:14,15 completed (1) 23:19 completely (1) 77:17 complexity (1) 11:20 complied (1) 39:7 compliment (1) 17:13 compromise (2) 8:14;12:11 compromised (12) 8:10;12:20;15:21;24:9; 47:21;53:15;55:11;57:5; 58:2;59:16;63:7;69:19 compromising (1) 12:16 computer (29) 14:11,12,15,17;15:6,19; 16:17,18;17:4;20:7;38:15; 47:14;53:18,21;71:3;75:4,7, 8,14,16,17;76:10;78:1,8,12, 14;79:2,11,16 computers (12) 14:6,7,8;16:16;28:12,21; 31:8;38:15,18;76:4,8;77:7 concerns (1) 53:13 concluded (4) 35:17;51:21;62:9,19 conclusion (2) 35:17;75:18 conclusions (2) 45:7;60:8 conduct (2) 13:4;47:13 conducted (9) 29:3;45:6,8;47:16;56:2; 61:17;62:21;65:21;66:2 conducting (4) 20:13;30:6;42:4;43:13 conduit (1) 63:11 conference (3) 6:19,21;7:14 confidence (2) 26:17;27:16 confidential (3) 18:6,8;19:20 confinement (1) 60:14 confirm (1) 56:5 confirmed (3)
---	---	---	---

33:15;50:2;56:20 Congress (1) 54:6 connected (2) 28:13;75:16 connecting (2) 16:15;79:16 connection (2) 14:13,14 connections (1) 77:8 consequences (1) 9:19 Consider (2) 20:21;35:5 considered (3) 11:4,10;45:16 consolidate (1) 41:12 constant (4) 30:4,4;50:7;55:15 contact (4) 15:11;28:6;46:9,11 contacting (1) 63:2 contained (6) 15:20;26:15;38:16;72:14; 73:9;80:16 containing (2) 46:9;49:9 context (1) 58:18 continue (1) 51:20 continued (4) 62:20;65:16,19;66:17 continuing (1) 40:15 contractors (1) 31:7 contributing (1) 40:12 control (3) 19:2,15;59:2 controlled (1) 64:3 conversations (1) 35:19 convoy (1) 37:17 convoys (1) 42:20 Coombs (10) 5:17,18;6:9,16;7:5,13; 69:14;70:1,5;81:8 copy (9) 6:14,16;15:16;28:10,15, 19;29:5;71:3;74:11 Corp (1) 54:5 corrected (1) 15:13 corrective (1)	33:14 correlating (1) 62:17 correspond (1) 65:3 corresponding (1) 50:5 counsel (1) 6:18 counted (1) 62:16 counter-intelligence (3) 50:14;51:2,8 country (4) 9:5;33:1,7;34:1 couple (1) 9:1 COURT (39) 4:2,2,5,17,18,21;5:1,14, 17;6:5,8,10,12,12;7:1,5,10, 15,16,18,18,19;8:2;13:14; 52:20;69:5,11;70:1,6,6,9,9, 10,11;72:3;75:20;81:6,9,9 courtroom (2) 4:10,11 Court's (2) 5:21;6:7 covering (1) 14:18 cracking (1) 17:3 create (3) 40:9;41:17;58:8 created (10) 33:19;38:8;46:14;48:21; 50:8;52:16;53:20;54:11; 75:6;77:12 creates (1) 53:21 credit (1) 22:10 crime (1) 59:12 crimes (3) 13:20;14:19;38:3 criminal (2) 25:19;27:13 crisscrossing (1) 16:14 criteria (1) 61:9 criterion (1) 18:15 critical (2) 20:16;24:8 critiques (1) 61:15 crypt-ed (1) 75:12 Crypto (2) 57:15,15 CSD (1) 9:6	current (4) 43:2,13,17,19 currently (1) 4:16 cyber (1) 29:7 D D6A (8) 30:15;31:2,3,5,7;38:15, 15;39:4 daily (3) 24:4;30:18;37:12 damage (2) 18:9;22:6 damaging (1) 10:5 dangers (2) 26:2;51:10 darkness (1) 68:4 data (16) 15:3,4;16:12,13;30:15; 40:20;41:19;42:3,8;43:13; 45:6;46:1;53:17;63:21; 69:19;77:6 database (4) 31:17;39:11;40:1;69:2 databases (7) 15:17;42:2,5;45:21;50:4; 63:6;64:17 dataset (1) 70:12 date (6) 14:19;15:4;53:18;67:7; 76:20;77:3 dated (8) 5:3,6,9;16:1;33:18;52:8; 54:3;71:3 dates (5) 34:6,11,17;77:13;79:4 day (8) 10:2;21:4;30:17,19; 47:20;48:2;49:5;79:7 days (5) 47:17,19;48:20;77:15,17 DE22PAXzip (1) 72:13 dealt (1) 37:11 December (30) 16:1,1,7;32:1;46:21;47:7; 50:19;54:6;62:11;65:2,17, 20;66:1,15;67:1,5;68:10; 71:3,19,21;72:6,9;73:16,17; 75:7,19;76:16,19;80:8,9 decisions (4) 18:14;21:9;42:16;44:2 deck (1) 21:7 declassification (1) 19:7	decreased (1) 42:13 decrypting (2) 71:7;75:9 decryption (2) 72:1,11 defeat (2) 32:2;38:8 defense (17) 5:3,19;6:11;7:6;34:12; 44:8;50:5;55:9;60:4;63:9; 64:11,12,12,18;71:8;78:3; 80:15 definition (1) 34:2 deleting (1) 14:18 deliberate (1) 33:5 deliberately (4) 12:10,20;59:15;67:7 deliberations (1) 14:5 delineated (1) 35:11 delivered (2) 8:16,18 Delta (3) 53:12;66:10,11 demonstrate (1) 12:9 demonstrated (1) 62:5 Department (5) 16:11;34:11;48:1;55:8; 62:15 deployed (7) 8:3,7;38:1,6;45:4;48:11; 60:10 deployment (3) 10:4,10;66:18 Deputy (1) 80:19 described (3) 53:10;56:21;68:17 describing (1) 10:1 description (1) 35:1 designations (1) 18:6 designed (2) 36:14;38:18 desired (1) 43:19 destinations (1) 77:8 destroyed (1) 8:13 destroys (1) 71:10 destruction (1) 28:14
---	--	---	---

detailed (2) 53:11;68:12	42:10;73:10	9:12;14:1,4;16:7;19:17; 27:20;32:9;33:12;47:2;80:5	ending (1) 16:18
details (1) 73:13	disprove (1) 71:9	duties (1) 17:11	enemies (12) 10:15;20:17;21:11;23:4; 28:1,12;29:16;32:20;33:6; 36:1;43:7;60:2
detainee (5) 65:17,20;66:5,7,14	disseminate (1) 40:6	E	enemy (33) 8:17;10:18;11:1,1;13:9; 20:12;22:4,14,20,21;31:19; 37:20;38:8;40:12,19;41:1,5, 13;42:9;43:5,6,9,10,10,14, 21;44:7,11,20;45:3,4,8
detection (1) 20:15	dissemination (1) 39:6	early (4) 16:13;67:1;68:9;73:15	enemy's (2) 44:11,16
determine (2) 42:12;68:14	distant (1) 43:3	easily (1) 29:4	engine (1) 39:16
detriment (1) 12:5	diverse (1) 55:18	easy (1) 28:6	enough (1) 32:19
device (1) 15:10	division (1) 40:7	editorial (1) 58:5	ensure (2) 60:1;67:20
devices (1) 37:5	divulging (1) 35:6	editors (1) 63:2	enter (1) 36:18
devoted (2) 64:15,16	doctrine (1) 15:12	education (1) 12:4	entered (1) 37:3
die (1) 68:5	document (18) 18:17;25:15;30:19;50:12, 16;51:2;52:19;53:16;54:11, 12,14,15;55:12;58:7;68:15, 16,19;80:1	effort (2) 72:2,11	enterprise (5) 56:7;59:11;60:21;61:2,10
difference (1) 61:3	documentaries (1) 35:14	Ehresman (3) 43:1,12;67:6	enterprises (1) 60:18
different (7) 16:15;19:13,19;23:5; 37:15;56:9;74:19	documentary (1) 13:14	eighth (1) 16:20	entire (4) 15:16;21:7;41:8;79:8
difficult (1) 68:13	documents (15) 8:15,16,19;19:4,4;25:8, 15;27:19;51:13;52:10;57:6; 58:11;59:11;64:16;72:18	either (2) 6:15;79:5	entirely (2) 49:20;61:14
digital (2) 19:18;20:1	DoD (5) 24:3;51:12,18;52:2;58:2	electronic (1) 37:5	entitled (1) 28:16
diplomats (1) 34:12	dog (1) 9:1	elements (1) 55:19	entry (1) 77:21
direct (1) 55:10	domain (2) 57:21;58:16	elicited (1) 17:2	environment (1) 38:6
discipline (1) 13:5	donors (1) 64:4	Elisa (1) 25:21	escort (1) 36:18
disclose (5) 21:10;25:12;27:18;64:8; 67:21	down (3) 31:4;40:7;68:5	else (2) 7:11;49:15	essential (1) 44:1
disclosed (2) 57:18;59:16	download (1) 79:21	email (4) 6:16;20:20;21:1;59:6	essentially (3) 39:5;51:9;61:7
disclosing (3) 11:15;67:3;71:13	downloaded (7) 53:1;54:12;79:8,11;80:1, 5,8	Emeker (1) 30:2	established (1) 59:11
disclosure (1) 55:7	downrange (1) 32:4	employ (1) 43:15	evaluation (2) 17:19;56:20
disclosures (4) 15:18;20:19;35:18;48:16	draft (1) 61:16	employed (3) 39:8;42:8,18	even (9) 20:6;34:12;36:19;39:2; 44:10;57:4;61:8;67:6;71:16
discover (1) 20:13	draw (1) 42:14	employee (1) 71:2	evening (1) 7:4
discredit (1) 13:6	drive (9) 15:10;28:3,19;29:11,19; 32:16;33:13;46:11;78:6	employees (1) 24:15	Event (4) 58:17;67:5,5;71:11
discuss (3) 7:1;15:13;20:20	drown (1) 42:14	employer (1) 75:6	eventually (1) 24:19
discussed (4) 38:6;49:17;53:6;55:2	Drum (2) 31:10;32:3	enable (1) 40:20	everybody (1) 81:7
discusses (1) 58:2	duly (1) 80:20	enabled (1) 41:1	Everyone (1) 36:16
discussing (3) 54:5;57:4;59:5	duplicate (1) 75:3	enables (1) 39:17	evidence (27) 9:7;11:17,21;12:3,18;
disgruntled (1) 24:15	during (10)	enabling (1) 29:14	
disk (1) 20:2		encrypted (3) 71:4;75:16;78:17	
display (2)		end (1) 11:6	

13:2,8,14,18,21;14:3,3,19; 15:8;16:2,20;17:1;29:11; 33:3;45:16;48:18;62:2,4; 63:10;71:9;75:20;76:3 evidenced (1) 28:1 exact (2) 33:9;67:6 exactly (2) 55:17;59:19 examination (1) 33:12 examined (1) 76:5 examiner (1) 76:2 examiners (1) 14:21 example (3) 22:2,6;62:8 examples (1) 28:21 exclusively (1) 63:14 executed (1) 26:18 Executive (1) 18:12 Exhibit (67) 5:9,12;6:2;16:21;17:1,17, 17;18:2;20:4,10;21:7; 22:18;23:19,20,21;24:12; 26:20;27:3;28:4,7;33:17, 18;46:7;47:12,12,15;49:3; 50:3,5,15,17,21;51:4;52:10, 17,20,21;53:3,17;54:9,10; 55:5,14;56:13;58:9;64:11, 12,12;65:1,10;68:7;73:3,4, 19;74:11,14,18;75:10; 76:15;77:11,12,18;78:20; 79:2,13,15,17 exhibits (3) 5:1;64:17,18 expected (5) 13:16;26:1;39:15;44:14; 73:12 experience (1) 32:14 expert (3) 5:7;44:9;60:5 experts (1) 72:21 explain (4) 12:3,7,12;71:11 explained (7) 14:1;21:15;22:7;26:11; 39:19;42:12;43:1 explanation (1) 75:21 exploitation (1) 39:6 exploited (1) 41:7	exposes (1) 26:6 exposure (1) 31:10 external (1) 29:10 external (10) 15:9,10;24:14;28:3,19; 29:19;32:16;33:13;46:11; 55:7 extracting (1) 11:14	file (32) 7:3;15:21;28:7;46:8,13; 53:19;54:1;55:13;70:17; 72:13,14,14,15;73:4;75:5, 16;78:4,7,9,11,12,17,19,19; 79:1,4,10,10,12,12;80:12,13 filed (3) 5:1;6:17;22:5 files (4) 75:9;76:17;79:5,11 Finally (4) 13:7;17:4;20:18;51:21 find (2) 11:8;76:3 Finding (3) 6:11;32:5;67:3 findings (1) 31:13 fine (1) 6:8 finished (1) 46:19 finishing (1) 70:3 fire (3) 30:7,7;42:20 fired (1) 48:6 firewall (1) 16:11 firewalls (1) 16:3 first (26) 11:4;12:2;13:19;14:6; 20:10;25:2;30:1,2;31:6,9; 38:10;41:11;46:21;47:21; 48:4;50:13;51:5;52:11; 56:15,21;67:10;69:19; 70:12;74:1;76:1;77:2 first-class (1) 31:15 firsthand (2) 61:20;63:3 fish (1) 10:5 five (7) 47:17,19;48:20;50:18; 70:7;74:12,16 fix (1) 55:1 flag (1) 10:11 flawed (1) 60:7 flow (1) 16:13 FOB (7) 32:13;36:12;38:11,12; 47:18,19;78:6 focus (3) 32:9;40:13;43:20 focused (8) 30:3;34:2;40:13;48:9,10;	50:9;65:6;72:21 focusing (1) 12:14 FOG (1) 40:11 FOIA (1) 6:3 folder (4) 53:19;73:6;76:17;78:5 folders (1) 74:19 follow (2) 11:21;62:20 followed (1) 6:7 following (2) 22:2;35:19 force (1) 51:7 forced (1) 13:6 Forces (3) 45:4,10;51:16 forefront (1) 14:4 foreign (11) 9:20;18:18;21:11;35:7; 42:1;51:13,14,15;52:1; 68:14,14 forensic (5) 14:19,21;33:12;76:2,10 forensically (4) 14:17;46:8;73:14;76:9 form (2) 59:18;63:6 formal (4) 12:4;17:16;29:20;32:1 formally (2) 23:7,10 format (2) 9:6;41:21 forms (1) 35:19 forward (1) 58:19 found (8) 9:15;20:2;33:13;45:20; 46:8,8;53:2;75:5 four (2) 47:16,18 Fourth (2) 15:15;78:20 Fox (1) 24:20 Foxtrot (2) 64:12,18 free (2) 36:2;58:16 Freedom (1) 58:19 friendly (1) 31:20 front (1)
	F		
	facilities (1) 34:15 facility (1) 36:14 fact (2) 9:1;13:17 facts (3) 59:14;71:7,12 failed (1) 61:8 fame (1) 67:16 family (1) 34:16 far (1) 56:12 Farrah (1) 80:2 fast (1) 48:17 faulty (1) 62:9 fear (1) 55:10 February (9) 48:12;49:1;53:2;54:12; 77:1,5,9,19;78:2 Fein (13) 4:3,4,18;5:2,15;6:6,8;1; 52:21;69:8,17;70:11,12; 72:5 fellow (2) 34:20;37:18 few (3) 28:21;29:1;68:4 Field (7) 28:11,20;29:5;31:3; 39:13;40:7;44:9 Fifth (1) 15:19 fight (1) 45:11 fighting (1) 71:8 figures (1) 31:20 figure's (1) 59:6		

37:16 Ft (2) 31:10;32:3 full (4) 17:13;24:20;32:16;69:10 fully (1) 8:7 Fulton (5) 42:3,7,11,15;44:3 further (3) 28:18;35:11;62:19 fusion (2) 32:10;40:11 future (1) 43:3	14;18;12;19:2,9;25:11; 26:3,18;34:14;50:2,7,9; 53:14;55:21;57:2;59:1; 61:5;63:15;64:2;81:2 governments (2) 35:7;68:14 Government's (2) 5:10,12 grab (1) 22:9 granted (2) 17:10;25:1 grave (1) 70:2 grinning (1) 9:21 group (1) 58:19 groups (5) 22:17;34:11;35:5;43:14; 51:14 Guantanamo (3) 66:10,11,14 guarantee (2) 48:16;67:16 guiding (1) 17:5 Guilty (1) 6:12 guys (1) 31:12	15:20 head (1) 58:13 headquarter's (1) 36:13 heads (1) 73:10 heard (12) 13:14;20:1;38:4,21;40:8; 44:3,8,17;46:18;48:18; 74:3;78:4 heart (1) 9:7 heat (1) 68:5 held (10) 10:8;14:8,13,15;29:14; 33:4;35:6,12;36:7;54:6 help (1) 22:4 helped (1) 70:14 helping (1) 70:16 helps (1) 71:11 here's (1) 76:1 hey (1) 59:9 high (1) 34:12 highlighted (1) 25:11 highlighting (1) 34:10 highlights (1) 31:12 Hillary (1) 9:6 himself (5) 9:3,12;10:10;28:2;68:2 historic (1) 43:18 historical (2) 43:12,16 hold (1) 33:8 Honor (167) 4:4,7;5:2,11,15;6:6;8:1,2; 9:1,9,15,17;10:17;11:16; 12:2,7,12,17,21;13:2,7,12; 14:6,21;15:9;16:1,7,17,21, 21;17:4,8,18,20;18:5,10,15, 19;19:3,17;20:4,9,18;21:13; 22:16;23:7,16,21;24:6,12, 17;25:21;27:3,9,20;28:5; 29:9;30:1;31:1;32:2,12,18; 33:2,8,16,21;34:2,5,9,13,18; 35:9,16;36:3,10;37:8;38:4, 10,21;39:10,14;40:8,15; 41:10;44:17;45:2,13;46:4,7, 12,18;47:4,13,17,20;48:7,8,	18;49:15;50:13;51:5,17; 52:6,7,11,19;53:15;54:2,8, 9;55:11,15;56:1,12,14,19; 58:10,21;59:4,10,19;60:4,8; 61:7,11;63:8;64:5,14;65:7, 19;66:4,13,21;67:18;68:3, 17;69:3,21;70:5,19;71:8,10; 72:10,12;73:3,14,16;74:11, 13,13,21;75:4,10,15;76:1, 12,19;77:2,10;78:7,13,20; 79:13;80:4,7,9;81:1 hour (1) 69:15 hours (3) 66:21,21;69:10 housed (1) 76:15 human (2) 9:2;24:15 humans (1) 9:1 hundreds (3) 8:14;9:13;27:18
G	H	I	
gaps (2) 44:19;45:1 Garani (2) 15:20;70:20 garrison (1) 32:15 gather (4) 32:21;38:13;48:19;64:8 gathering (2) 35:1;41:20 gave (8) 6:13;12:4;33:9,10;37:9; 40:20;41:7;71:1 gear (1) 8:8 general (3) 11:5;56:16;60:18 generally (1) 42:5 Germany (1) 54:7 GITMO (4) 53:12;65:9;66:14,19 given (3) 22:4;26:9;29:15 giving (2) 13:9;57:10 gleeful (1) 9:20 Global (1) 16:19 goal (1) 58:8 goals (1) 56:9 Gollihood (1) 5:6 good (5) 10:2;13:5;44:4;69:3;81:4 Google (1) 39:17 go-to-guy (1) 41:19 Government (25) 5:7;6:1,5;7:3,21;11:10,	hackers (2) 24:16;35:8 Hall (2) 44:8,17 Hammer (8) 32:13;36:12;38:11,12; 40:11;47:18,19;78:6 hand (2) 26:14;62:11 handle (1) 25:12 handling (1) 31:4 hands (4) 36:8;37:19;71:21;72:11 happen (1) 43:3 happened (2) 59:13,19 hard (9) 15:10;28:3,19;29:11,19; 32:16;33:13;46:11;71:9 harder (1) 59:2 hardware (1) 31:4 harm (3) 8:9;22:10;80:17 Haven (1)	IA (1) 24:4 Iceland (8) 47:7;48:5,9,11,12,15; 49:7,14 identification (1) 23:2 identified (4) 14:7;25:9;56:15;64:7 identify (2) 43:7;54:19 identifying (2) 34:20;35:10 identities (1) 22:17 IED (4) 31:18;32:1,2,5 IEDs (4) 30:6,10,12;42:20 immediate (1) 43:3 impact (3) 24:10;58:7;61:7 imperative (2) 21:18;37:10 importance (3) 24:8;27:10;36:6 important (3) 20:11;43:13;70:21 importantly (1) 80:4 improperly (1) 25:12 inaudible (36) 16:10;20:17;37:14;39:9, 10;42:4,5,17;47:3;48:1; 49:8;51:1,8;54:14,18;59:8;	

60:5;65:1,6;70:13;71:5,19; 72:7,18,19;73:2,4;74:9,20; 75:3;78:4,5,11,13,21;80:19	61:1,6,7,8,12;63:6,12,16,20; 64:3,8,9;65:9;66:19;67:15, 16,19;68:1,11;71:14;73:9; 75:1;80:16	73:18	J
inbound (1) 43:2	informative (1) 32:16	intend (3) 12:7,12,17	
incident (1) 73:2	informed (1) 68:9	intends (2) 11:21;12:3	January (9) 9:12;14:18;47:8;54:3; 71:6;75:11,14;76:7,21
include (2) 23:1;34:6	infrastructure (1) 24:8	intent (1) 52:5	Jason (3) 71:2;75:4,5
included (5) 24:14;31:17;36:19;44:5; 68:19	initial (1) 41:6	intentional (1) 33:5	JC (1) 15:19
includes (2) 35:12;53:8	Initiative (1) 48:13	intentionally (3) 12:10,19;59:15	job (4) 30:3;37:12,13;42:1
including (12) 13:15;22:17;26:16;35:8, 14;37:1;45:14;55:3;60:2; 61:18;73:8;74:21	inside (2) 58:12,12	intentioned (1) 9:18	jobs (1) 38:5
inclusion (1) 69:1	insider (4) 45:20;55:8,8,9	interest (4) 8:5;50:1;55:20;57:3	Johnson (3) 46:8,13;76:2
incorrectly (1) 62:14	insight (1) 60:9	interested (4) 10:6,9;48:15;71:13	Johnson's (1) 33:12
increased (1) 42:13	installations (1) 34:15	internal (1) 24:14	joint (1) 32:2
independent (3) 29:2;61:17;63:1	installed (1) 38:18	internet (21) 13:4;21:17,18,21;22:9, 20;26:4,6;28:13,21;29:4,15; 32:21;35:14,20;36:8;52:8; 55:2;57:19;62:16;63:5	journalism (2) 56:11;61:3
in-depth (1) 44:15	instances (1) 28:17	interrogation (7) 65:12,13,14,18;66:1,11, 15	journalist (1) 57:7
indexdact (3) 79:1,4,15	instant (1) 40:5	interrogations (1) 65:9	journalistic (6) 56:6;59:11;60:17,21; 61:2,9
indirect (2) 13:10;30:7	Instead (1) 37:4	interview (1) 61:19	journalists (1) 35:20
indiscriminate (1) 8:14	instructed (2) 23:3;68:7	into (7) 15:6;30:19;42:1;53:21; 68:4;75:7,8	JRTC (4) 30:2;31:11;32:11,14
individual (6) 19:11;22:11;25:2,3; 34:16;55:10	instructing (1) 21:14	introduced (1) 15:6	JTF (1) 66:14
individuals (1) 29:2	instruction (1) 17:18	investigating (1) 73:1	judgment (1) 51:6
individual's (1) 22:11	instructor (1) 21:14	investigation (4) 16:10;72:19,21;79:8	Julian (20) 11:3;14:16;15:2;17:2; 45:18,20;46:9;47:9;48:6, 12;49:17,18,20;56:4,13,19; 57:9;61:15;64:1;68:6
infantryman (1) 37:16	Insurgent (2) 28:10;29:6	investigations (1) 74:19	July (5) 5:3,6,9;32:8;60:13
information (165) 10:5,8,15,19,20;11:13,14; 12:10,16,19;14:16;15:1,5,7, 11;17:6,20,21;18:3,6,11,16, 16;19:1,8,12,14,16;20:12, 16;21:10,17,18,21;22:3,8,9, 14;23:2,17;24:3,5,9,9,13; 25:1,4,9,10,12,14;26:4,6,7, 10;27:2,6,11,17;28:7;29:3, 10,12,14,14,15;30:5,9; 32:21;33:6;34:3,6,7,13,20; 35:7,12,19,20;36:7,8,15; 37:2,6,11,13,19;40:6;41:1, 4,9,15,16;42:8,15;43:16,17, 19;44:5,12,16,18,19;45:10, 18,19;46:9,12;48:1,20;49:4, 10,14;51:13,16,19,20;52:2, 8,18;53:8,11;55:3,4,9,17, 18;57:5,21;58:3,4,15,16,19, 20;59:2,3,6,7,16,18;60:1;	insurgents (2) 30:6;51:14	IP (1) 16:17	jumped (1) 23:15
	intel (5) 11:6;16:6;52:18;57:11; 74:2	Iraq (9) 8:13;15:11,16;23:11; 32:9;33:3;42:14,19;48:11	June (4) 33:19;35:9,17;36:5
	Intelink (6) 39:16,20;40:2;46:17; 64:21;66:19	IRR (11) 50:11;52:8,11,13,18;53:4, 6;54:11;68:9,17,19	junior (3) 44:10,12,14
	Intelinks (1) 47:5	Islandic (1) 48:13	K
	intelligence (62) 8:11;11:4,10;12:8;13:3,9; 14:9;17:10,12;21:5;24:17; 28:11;29:8,21;30:13,17,18; 31:16;32:15,17;35:1;36:5, 10;37:11,18;38:5,7,11,13, 19;39:1,3,5,18;40:17,18; 41:17,20,21;42:21;43:16, 20;44:9,19,21;46:2;49:9; 51:13;52:7,12,13;53:6; 55:16;56:8,15,17;57:1,2; 63:17,19;64:16;65:5	ISN (1) 66:19	
	intelling (1)	issue (1) 78:15	Katz (2) 71:2;75:5
		issues (2) 7:2;31:5	Katz's (3) 15:19;75:4,16
		items (2) 64:21;65:3	keep (1) 28:5
		Ivory (3) 25:21;26:11,19	keeps (1) 78:8
			kept (6) 28:9,10,15,19;29:5;67:18
			key (9) 12:2;13:21;14:3;15:7;

16:2,20;18:20;33:2;51:6 kind (1) 34:11 Kits (1) 39:4 knew (22) 10:21;11:1,2;12:9,15; 24:2,7,13,21;27:10;29:11; 36:7;40:18;44:10;48:14; 55:17;56:8;57:18;62:3; 67:16;77:15;80:10 Knowing (2) 20:14;59:17 knowingly (2) 13:9;27:14 knowledge (12) 8:9;12:5,13;29:13;32:20; 39:21;40:18;44:6;45:13; 61:20;62:7;63:3	leads (2) 43:11;74:20 leak (3) 11:12;55:9;68:15 leaked (2) 53:7;55:3 leaking (2) 68:16,19 leaks (1) 35:11 learn (1) 50:6 learned (9) 19:3,6,10,18;23:8,10,11, 13;27:20 least (2) 68:5;75:2 leave (4) 37:5;47:21;48:21;77:4 left (2) 37:3;47:2 legal (1) 74:1 lengthy (1) 69:20 less (6) 23:15;46:15;50:18;57:2; 64:19;79:8 lesson (1) 17:18 letter (1) 9:21 level (3) 22:3,7;81:1 light (1) 17:5 likely (1) 51:18 Lim (1) 37:9 limitations (1) 18:20 Line (14) 53:2,16;54:2,11,16;65:15, 20;66:1,3,8,16,20;77:18; 79:17 Lines (2) 65:18;66:7 link (2) 14:8;16:6 List (15) 16:19;17:5;50:3;57:11; 59:8;64:6,10,11,13,21;65:4, 11;66:4,9;67:19 listed (2) 73:5;78:11 lists (1) 35:4 litany (1) 25:7 little (1) 72:3 live (1)	36:2 lives (1) 24:11 locally (1) 79:5 locate (1) 31:12 located (6) 36:13;72:17;74:10;78:5; 80:3,13 location (2) 22:13;34:14 locations (1) 34:7 log (3) 52:18;53:21;76:16 logged (1) 15:7 logistics (1) 7:1 logs (23) 16:3,6,9,11,14;50:15; 56:3,5;71:1;76:14,14,19,20; 77:6,13,14,20,21;79:14,16, 18,20;80:5 Loma (1) 15:2 long (3) 6:6;8:17;69:15 longer (1) 69:5 look (4) 51:4;56:12;57:7;79:13 looked (1) 56:2 Looking (4) 10:4;55:12;64:9;69:7 lowest (2) 22:3,7 lunch (6) 69:7,9,12,16;70:4;81:5	maiden (1) 22:5 mail (1) 26:9 main (1) 61:12 mainly (1) 43:5 maintained (1) 14:9 Major (13) 4:3,4,18;5:2,15;6:6,8,1; 52:21;69:8,17;70:11,12; 72:5 making (2) 10:9;45:7 Manning (175) 8:3;9:2,11,21;10:3,13,18; 11:2,7,18;12:14,19;13:3,8, 19;14:20;15:21;16:14,18; 17:2,9,15;18:1,3,21;19:3, 21;20:5,10;21:8,14,20; 22:12,16,19;23:3,5,7,13; 24:7,13,18,21;25:6,15;26:2, 5,11,12,14,18,21;27:4,14, 20;28:2,5;29:9,19;30:8,13, 15,17,20;31:2,6,10,16; 32:10,12;33:3,9,16,20;35:4, 11;36:4,10;37:1,21;38:9; 40:10,16,20;42:8,18;44:4, 10;45:2,5,17;46:1,16;47:1, 5,7,14,21;48:4,8,14,19,21; 49:6,13,15,17;50:6,17;51:9; 52:4;53:1,15;54:12;55:11, 16;56:5,7,8,14;57:5,10,14, 16,18,20;58:1,10;59:1,7,15; 60:1,10,13,18;62:2;63:7,11, 16;64:1,19,20;65:8,13,16, 19;66:6,13,17,18,21;67:7, 11,14,19,21;68:3,9;70:16, 21;71:10,12,18;72:5;73:15, 17;74:1;75:1;76:10;77:2,4; 78:13,18;79:8;80:9 Manning's (35) 8:20;9:8;12:4,8,13;14:11, 12;15:9,15;16:4;17:5;20:3; 21:13;23:17;30:2;32:19; 33:13,14;34:2,9;38:6;40:9, 21;41:18;42:1;45:13;46:11; 56:2;70:13;75:17;77:7; 78:1,12;79:1,16 Manual (3) 28:11,20;29:5 many (3) 23:15;31:16;36:1 map (2) 41:16;42:10 March (5) 16:12;50:20;52:8;66:18; 76:8 Marine (1) 54:5 mark (2)
L			
label (1) 19:21 Laboratories (1) 15:20 laboratory (1) 75:6 labs (1) 71:2 lab's (1) 75:7 Laden (1) 23:9 Lamo (8) 46:5;49:2;56:4;58:10; 67:11;70:14,21;71:1 land (1) 72:10 lands (1) 71:21 language (1) 51:9 laptop (1) 14:12 large (3) 34:11;40:12;55:6 largely (1) 60:12 largest (1) 64:13 last (6) 4:5;6:16;7:20;69:19; 70:11;78:8 late (4) 8:3;16:12;67:1;73:15 later (5) 15:14;48:2;52:18;66:2; 80:9 lead (1) 75:18 leader (1) 46:10			
		M	
		Ma'am (4) 5:18;70:12;72:5;81:8 Mac (6) 15:7;53:20,21;71:20; 72:8;76:9 machine (2) 30:15;39:4 machines (1) 31:5 Macintosh (1) 20:7 Madaras (4) 31:1,1;32:7;39:19 Madrid (1) 33:15 magazines (1) 35:13 magnitude (1) 64:14	

19:4,18 marked (1) 19:5 Martial (1) 6:12 mass (5) 28:13;41:20;42:8;68:18; 72:1 material (4) 21:2;29:19;68:21;69:1 materials (2) 8:10;28:2 matter (3) 9:2;33:11;72:21 matters (1) 48:15 maximizing (1) 61:6 maximum (2) 4:15;58:7 may (5) 8:2;24:21;29:7;43:3; 54:21 maybe (1) 69:14 McIntosh (1) 14:12 mean (1) 18:7 meaning (1) 30:21 means (4) 13:10;29:4;46:20;78:13 meant (1) 10:11 measures (1) 19:15 media (7) 4:8,8,10;19:19;20:1; 48:13;62:11 meet (1) 61:8 members (6) 4:8,9;34:16;39:6,17; 41:18 merely (1) 59:21 messaging (1) 40:5 met (2) 6:18;29:3 methodology (1) 60:7 methods (4) 34:21;56:9;68:10,21 Microsoft (2) 28:9;78:7 might (2) 7:2;69:3 military (9) 9:20;18:18;22:1;34:4,15; 50:8;55:19;64:16;73:13 Miller (3)	31:14;36:19;42:15 mind (4) 8:20;9:8;14:4;45:20 mine (2) 42:8;49:20 mined (1) 30:13 mining (5) 29:7;30:16;41:19;42:3; 46:1 minus (1) 56:17 minute (3) 7:14;69:11;70:3 minute-by-minute (1) 16:5 minutes (2) 69:20;70:3 misinformation (1) 60:6 missing (2) 77:13,20 mission (5) 8:11;22:13;24:10;61:4; 67:2 mistrial (1) 5:4 mobile (1) 32:1 model (1) 62:20 Modern (1) 48:13 Moiser (1) 74:7 Mole (4) 21:13,20;22:19;23:3 moment (1) 28:8 Monday (1) 7:9 moniker (1) 49:2 monitoring (1) 54:5 month (1) 66:2 months (2) 10:3;60:13 more (14) 10:5;13:13,15;14:2;46:3; 47:6;49:13,14;57:7;59:3; 65:21;69:9,10;72:3 morning (2) 4:8;7:9 Morrow (1) 4:6 Most (14) 17:4;43:17;50:3;51:18; 64:6,10,13,21;65:3,11;66:4, 9;67:19;80:4 mother's (1) 22:4	motion (8) 5:3,19,20,21;6:4;7:4,6,9 motions (1) 6:11 Mountain (3) 27:6;36:12;46:20 mounting (1) 15:3 movement (3) 23:2;60:21;73:8 movie (1) 72:15 moving (1) 37:2 much (7) 22:6;42:18;45:18;62:13; 63:12;67:15;69:5 multiple (5) 12:20;16:3;17:14;72:20; 73:7 must (8) 20:14;24:3;34:10,21; 35:18,21;51:21;80:7	needing (1) 68:4 needs (1) 56:12 net (1) 16:13 network (1) 60:5 networking (1) 35:15 networks (1) 67:12 new (2) 49:16;59:12 news (9) 35:13;49:12;60:12;61:12; 62:6,10,17,17;63:1 newspapers (2) 35:13;63:2 next (6) 28:6;69:12,15,18,21; 79:17 night (1) 6:16 NIPRnet (1) 45:21 nondisclosure (8) 25:5,7,18;26:16,21;27:4, 10,15 None (1) 65:4 nor (2) 61:19;62:4 normal (1) 40:17 note (5) 40:19;51:5,5;74:13;77:10 noted (1) 56:20 notice (3) 18:21;31:7;75:1 notoriety (2) 8:19;9:5 November (11) 46:14,14,20;65:2,2,8,15; 66:7;67:1;73:15,17 NT (2) 78:11,18 number (3) 22:5;23:14;38:4
		N	
		naive (1) 67:4 name (10) 10:9;11:12;22:4,5,10,13; 53:19;64:9;72:13;80:12 named (2) 75:5;78:5 names (2) 34:16,19 narrative (1) 71:10 nation (1) 36:9 national (13) 8:5;15:20;18:9;24:10; 26:7;34:4;45:11;50:10; 52:14;55:20;71:2;80:15,17 nationals (1) 21:11 nations (1) 29:2 nation's (1) 36:1 NCIS (1) 50:11 NCOs (1) 34:12 NDA (2) 26:12,19 NDAs (1) 37:21 neatly (1) 29:9 need (4) 7:11;25:3;41:6;75:13 needed (3) 4:14;44:7;71:6	oath (1) 8:4 oaths (1) 10:6 OB (1) 24:5 objection (4) 6:5,7;70:2,5 objectives (1) 67:9

<p>obligation (1) 27:7</p> <p>obligations (1) 10:6</p> <p>observed (1) 48:4</p> <p>obtain (4) 27:1,5,17;63:12</p> <p>obtaining (1) 59:5</p> <p>obvious (1) 45:17</p> <p>occasions (1) 50:18</p> <p>occurred (1) 75:19</p> <p>occurring (2) 30:10;58:18</p> <p>October (1) 8:3</p> <p>off (1) 24:2</p> <p>offenses (1) 5:5</p> <p>offered (1) 60:4</p> <p>office (2) 39:8;74:8</p> <p>officer (1) 44:6</p> <p>official (5) 34:7;37:7;52:9;53:8,13</p> <p>offset (1) 15:13</p> <p>often (2) 30:10;42:7</p> <p>once (4) 6:10,21;53:20;76:21</p> <p>one (12) 4:9;14:2;21:4;24:2; 30:19;33:2,15;47:20;67:2, 10;69:8;75:18</p> <p>online (2) 68:11;69:1</p> <p>only (18) 8:7;9:2;24:21;26:6;34:7; 37:7;52:9;53:9,13;55:7; 56:12;57:3;62:16;67:2,5; 71:13;74:2;76:20</p> <p>on-the-job (1) 29:20</p> <p>onto (1) 62:15</p> <p>open (6) 36:2;49:1,8,16,18;50:1</p> <p>opened (3) 78:9,13,17</p> <p>opening (1) 14:1</p> <p>openness (1) 58:9</p> <p>operate (2) 43:7,14</p>	<p>operated (2) 10:20;62:5</p> <p>operating (3) 16:4;66:10,12</p> <p>Operation (2) 4:9;57:10</p> <p>operational (4) 20:20;34:1;63:21;73:8</p> <p>operations (3) 20:14;30:4;66:14</p> <p>opinions (2) 60:11;62:1</p> <p>OPSEC (5) 34:2;35:11,21;51:8,10</p> <p>oral (3) 7:6,7,8</p> <p>order (16) 4:2;6:7;7:18;11:20;12:18, 21;13:5;18:12;19:16;27:1, 5,16,18;40:16;45:19;70:9</p> <p>orders (1) 64:14</p> <p>organization (8) 11:11;32:3,4;46:2;55:18; 61:4;62:4;63:11</p> <p>organizations (4) 23:6;29:2,7;59:2</p> <p>organize (3) 41:3;42:2,10</p> <p>organized (1) 29:9</p> <p>organizing (2) 41:15,21</p> <p>original (2) 56:21;80:20</p> <p>originally (1) 40:1</p> <p>Osama (1) 23:8</p> <p>OSC (3) 49:6,13,19</p> <p>others (4) 33:10,10;36:6;66:15</p> <p>out (6) 10:11;19:8;22:10;37:2; 42:2;59:4</p> <p>outcome (1) 10:16</p> <p>outing (1) 57:12</p> <p>outline (2) 13:2,7</p> <p>outside (3) 37:5;62:6;63:1</p> <p>over (6) 7:4;23:13;41:13;42:13; 43:15;62:15</p> <p>Overall (1) 69:9</p> <p>overflow (2) 4:11,14</p> <p>oversight (1) 58:5</p>	<p>own (13) 9:4;11:2;12:14;15:12; 22:2;34:9;44:12;45:9;46:4; 56:16;60:19;67:9;68:13</p> <p>owned (2) 19:1;25:10</p> <p>owners (1) 54:21</p>	<p>62:14</p> <p>period (3) 41:14;42:19;73:16</p> <p>permitted (1) 25:8</p> <p>person (5) 22:9;24:21;25:4;63:3; 71:21</p> <p>personal (12) 14:11;15:7;20:6;21:1; 28:21;37:4;53:20;61:16; 71:20;72:8;76:7,9</p> <p>personnel (1) 34:4</p> <p>pertaining (1) 48:15</p> <p>pertinent (1) 10:4</p> <p>Pfc (204) 8:3,20;9:2,8,11,21;10:3, 13,18;11:2,7,18;12:3,7,12, 14,19;13:3,8;14:11,12,20; 15:9,15,21;16:4,14,18;17:1, 5,8,14,21;18:3,21;19:3,21; 20:2,5;21:8,13,14,20;22:12, 16,19;23:3,4,7,13,17;24:7, 13,18,21;25:6,15;26:2,5,11, 12,13,18,21;27:4,14,20; 28:2,5;29:9,19;30:2,8,13, 15,17,20;31:2,6,9,16;32:9, 12,19;33:3,8,13,13,16;34:2, 9,35;4,11;36:4,10;37:1,21; 38:6,8;40:9,10,16,20,21; 41:18;42:1,8,17;44:3,10; 45:2,5,13,17;46:1,10,16; 47:1,5,7,13;48:8,14,18,21; 49:5,13,15,17;50:6,17;51:9; 52:4;53:1,15;54:12;55:11, 16;56:2,5,7,8,14;57:5,10,14, 16,18,20;58:1,10,21;59:7, 15;60:1,9,13,18;62:2,6,3,7, 10,16;64:1,19,20;65:8,12, 16,19;66:6,13,17,18,21; 67:7,11,14,19,21;68:3,9; 70:13,16,21;71:10,12,18; 72:5;73:15,17;74:21;75:17; 76:10;77:2,4,7;78:1,12,13, 18;79:1,8,15;80:9</p> <p>phase (1) 5:11</p> <p>phone (2) 57:15,15</p> <p>photos (1) 66:6</p> <p>physical (1) 13:13</p> <p>pick (1) 31:11</p> <p>picture (6) 9:9,9,10,11,14,17</p> <p>piece (5) 15:8;16:2,20;22:21;33:2</p> <p>pieces (2)</p>
		<p>P</p>	
		<p>packaged (2) 41:4,7</p> <p>page (23) 21:1;46:5;49:20;55:5; 56:14,19;57:7,11,12,15; 58:13,16,20;59:4,9;61:16; 68:6;71:1;74:9,12,13,17; 75:13</p> <p>pages (1) 74:15</p> <p>panel (1) 4:10</p> <p>Papa (2) 64:12,18</p> <p>paralegal (1) 74:7</p> <p>parochial (1) 57:2</p> <p>part (2) 72:18;81:3</p> <p>particular (5) 20:11;31:18;39:11;41:12, 20</p> <p>particularly (2) 42:9;54:20</p> <p>parties (6) 4:3,4;6:13;7:1,19;70:10</p> <p>pass (1) 76:10</p> <p>passed (1) 24:7</p> <p>password (3) 17:3,3;71:17</p> <p>past (2) 23:14;58:4</p> <p>patten (1) 30:11</p> <p>pattern (1) 31:18</p> <p>patterns (1) 43:7</p> <p>PE (1) 65:15</p> <p>PE81 (1) 65:18</p> <p>Peninsula (1) 29:17</p> <p>Penninsula (1) 13:11</p> <p>people (1) 57:1</p> <p>percent (1)</p>	

<p>13:13,21 piecing (1) 44:12 PII (1) 63:21 PIR (1) 44:18 place (2) 8:5;19:15 placed (2) 26:17;60:13 plan (3) 14:20;17:19;22:14 plans (2) 17:18;18:18 platform (2) 8:17;59:21 play (2) 24:3;43:4 played (1) 38:9 please (5) 4:3;8:2;40:19;45:18;51:5 pledged (2) 26:21;27:5 plot (1) 41:16 plug (1) 75:7 point (10) 51:5;61:21;74:9,10; 76:14;77:9;79:9,16,18;80:1 policy (1) 9:20 political (3) 31:20;58:7;61:6 poor (1) 62:7 port (1) 78:2 portal (2) 54:16;74:12 portion (2) 12:1;15:16 posed (2) 51:3;60:17 poses (1) 50:10 position (1) 26:10 posses (1) 55:6 possession (3) 19:8;29:10;51:19 possible (3) 11:7;45:18;48:17 post (4) 51:20;59:12;60:12;68:11 posted (5) 6:4;29:15;52:3;54:15; 61:16 posting (6) 20:21;22:3;35:20;52:9;</p>	<p>59:7,8 posts (1) 58:4 potential (3) 25:11;51:7;54:19 potentially (1) 51:15 PowerPoint (1) 28:9 PPI (1) 23:1 precise (1) 27:13 precisely (1) 46:3 predicting (1) 43:9 predictive (6) 40:13;43:5,8,11,21;44:15 prejudicial (1) 13:5 prepared (4) 6:11,15;42:14,19 preparedness (1) 73:13 present (7) 4:5,6,20;7:19,20;70:10,11 presentation (1) 33:14 presented (3) 17:16;21:7;33:15 presentencing (2) 5:8,11 presumed (1) 52:1 pretrial (1) 60:14 prevent (1) 20:19 previous (1) 32:11 previously (1) 17:8 primarily (1) 38:12 principled (1) 57:1 principles (1) 24:4 printout (1) 55:13 prior (4) 10:10;14:19;75:19;80:8 priority (1) 44:18 Private (5) 13:19;20:10;47:21;48:4; 73:21 probably (3) 69:8,18,19 procedures (2) 66:11,12 proceed (2)</p>	<p>7:12,21 PROCEEDINGS (1) 4:1 process (9) 6:1;18:10;19:7;38:9; 40:10;41:11,19;43:1;62:9 processing (1) 39:5 produced (2) 19:1;64:6 product (6) 12:8;30:11;36:3;43:1,20, 20 products (2) 38:7;40:9 professionals (1) 52:12 Professor (13) 60:4,6,9,11,16,20;61:9, 11,17;62:1,8,21;63:8 program (2) 17:18;38:16 programs (5) 35:13;38:15,18;39:7;40:3 prohibitions (1) 18:19 Propaganda (1) 28:10 proper (1) 18:13 properly (3) 19:4,18;80:21 proposed (1) 5:16 Prosecution (58) 16:21;17:1,17,17;18:1; 20:4,9;21:7;22:18;23:19,20, 21;24:12;25:19;26:20;27:3; 28:3,7;33:16,18;46:7;47:12, 12,15;49:3;50:3,15,16,21; 51:4;52:10,17;53:16;54:8, 9,55;5,13;56:13;58:9; 64:10,17;65:1,10;68:7;73:3, 19;74:11,14,18;75:10; 76:15;77:10,12,18;78:20; 79:2,13,15 protect (17) 8:5;10:7;19:12,16;20:11, 14,17;24:5;34:6,10,12,19, 21;35:21;37:13;68:8,8 protected (2) 23:1;71:17 protecting (5) 27:11;34:1,14,16;36:6 protection (3) 24:8;34:3;51:7 protective (1) 8:8 prove (2) 13:8;32:19 proves (1) 33:4 provide (3)</p>	<p>37:16;51:13;63:17 provided (2) 10:21;41:4 provides (3) 33:21;60:7;68:20 providing (2) 49:12;55:17 proving (1) 13:3 public (10) 11:5;34:3;35:19;48:3; 53:9;56:16;57:21;58:16; 59:6;81:3 publications (1) 49:11 publicly (3) 53:7;55:2;67:17 publish (2) 5:20;64:2 published (6) 6:1;13:4;48:2;53:9;55:4; 57:19 publishing (1) 53:11 pull (4) 30:8;41:9,11;42:2 pulled (2) 45:6,17 pulling (1) 44:5 purported (1) 63:5 purpose (8) 26:12;35:6;42:11;51:1; 52:13;53:4;54:19;61:6 purposes (1) 37:7 pursuit (1) 67:9 put (11) 6:3;18:21;20:5;21:21; 22:8;30:9;31:6;43:10;48:6; 53:21;74:21 puts (1) 26:8 putting (2) 26:3,5 Pv2 (1) 33:19</p>
			Q
			<p>qualified (1) 44:9 quick (1) 70:2 quickly (2) 40:5;63:4 quote (2) 11:5,6</p>
			R

R&R (3) 47:21;48:21;77:4	5:4;6:17	17:7;22:13;48:3;53:12; 59:18;63:4,12;67:17	8:17;33:19;62:6
raise (2) 52:14;53:4	record (3) 6:19;7:19;70:10	released (4) 45:19;52:5;58:3;62:15	resource (1) 11:2
raised (1) 26:14	records (2) 79:4,4	releases (2) 51:12;62:21	response (2) 7:3;48:3
ramification (1) 25:11	recount (1) 12:2	releasing (2) 33:5;36:7	responsibilities (3) 17:11;26:15;32:11
range (2) 28:12;31:4	recounted (1) 21:14	relies (1) 41:2	responsibility (3) 19:11,11;37:5
ranked (1) 42:2	recover (1) 15:1	remain (1) 14:4	responsible (4) 31:4;37:1;40:11;68:15
ranking (1) 34:12	recoverable (1) 76:6	remaining (1) 12:1	responsibly (1) 62:10
rather (3) 67:7;69:16;71:12	recruiting (1) 23:11	remember (2) 17:16;21:3	rest (1) 14:14
raw (1) 52:13	red (3) 20:19;74:15,15	remembers (1) 67:6	result (3) 10:17;25:19;27:12
RCM (1) 6:19	redacted (1) 62:11	remnants (1) 76:3	resulted (1) 10:14
reach (1) 42:1	redeploy (1) 42:14	remotely (1) 79:5	retained (1) 28:2
read (6) 6:18;7:10;19:4;31:11,16; 58:2	redirects (1) 74:2	remove (1) 37:6	retention (3) 65:13,14,17
reader (1) 64:7	reference (2) 28:6;29:18	repeatedly (1) 58:2	returning (2) 47:20;48:21
readily (2) 38:17;45:15	referenced (2) 54:4;78:3	repercussions (1) 55:10	revealed (1) 9:4
reading (2) 6:3;21:2	references (1) 32:17	report (22) 50:11,14,17,21;51:6,21; 52:12,12;53:2,10;54:3,4,4, 8,19;55:1,6;58:1,6;62:6; 68:9,12	revealing (1) 62:2
ready (3) 7:21;8:16;41:7	reflect (1) 7:19	reported (3) 55:19;62:14;77:19	reveals (1) 73:13
real (1) 48:16	reflected (1) 79:10	Reporter (2) 4:18;5:1	revelation (1) 57:3
realized (1) 63:4	regard (1) 5:18	reporting (2) 30:18;62:7	review (4) 52:1;55:16;60:12;74:13
rear (1) 37:17	regardless (2) 60:8;63:8	Reports (13) 9:14;30:21;31:11;39:12; 49:9;50:9;52:4;55:16; 61:19;62:17,18;63:1,19	reviewed (2) 61:13;76:13
reason (4) 20:18;21:3,16;77:5	region (1) 41:13	representative (1) 31:3	reviewing (1) 30:5
reasonable (1) 75:21	regular (1) 64:20	represents (1) 51:7	rifle (1) 8:8
reb (1) 21:3	regularly (2) 38:16;39:12	reputation (1) 22:11	right (15) 4:17,21;6:8,10;7:15; 26:14;45:20;46:4;47:2; 69:3,5,18;70:1,15;81:6
recalled (1) 48:5	Regulation (4) 18:4;19:14;28:15,16	request (3) 5:19;6:17;7:6	rip (1) 46:19
receive (3) 10:19;40:6;58:5	Regulations (1) 18:13	requested (1) 36:17	risk (1) 26:9
received (10) 17:13,16;18:1,3;21:4; 24:1;29:20;31:21;59:18; 61:15	reimaged (1) 76:8	required (11) 24:18;25:13,16;30:4,8, 20;31:11;34:19;36:16,18; 42:5	roadmap (2) 12:1;33:21
recent (1) 51:11	relate (1) 48:11	requirements (2) 5:21;44:19	Robert (1) 4:19
recess (11) 7:15,17;69:4,7,9,12;70:3, 6,8;81:5,9	related (7) 26:7;30:5;47:8;52:18; 65:9;67:2;78:21	research (6) 12:14;30:4;56:1;58:19; 61:18;63:1	role (3) 24:3;38:8;40:9
recessed (3) 4:5;7:20;70:11	relates (3) 13:20;53:1;80:15	researched (3)	room (1) 6:3
recognized (1) 34:18	relating (2) 42:9;46:2		rotation (2) 30:2;32:9
reconsideration (2)	relations (1) 18:18		rotations (1) 32:14
	relationship (3) 45:14,15;65:4		routine (1) 24:4
	release (8)		

<p>rule (2) 6:11;30:18</p> <p>ruled (1) 6:13</p> <p>Rules (1) 6:12</p> <p>ruling (3) 6:14,18;7:10</p> <p>running (1) 76:4</p>	<p>73:17</p> <p>searches (12) 16:6;47:11,13,16,18; 48:11;50:7;55:15;65:2,21; 73:21;74:2</p> <p>searching (6) 48:9;65:8,16,19;67:2,18</p> <p>Second (9) 14:11;27:4;32:9;42:21; 43:4;46:20;51:11;52:7; 76:12</p> <p>secret (15) 18:7,7,8;19:20,20;20:3,4, 8;24:18,19;36:17;74:16; 80:14,18;81:1</p> <p>secrets (1) 36:1</p> <p>Section (11) 36:11,12;37:10;39:7; 64:13,15,16;69:9,15,20,21</p> <p>secure (1) 57:16</p> <p>security (20) 8:5;17:21,21;18:4,9;22:5; 24:10;25:2;26:7,8;34:1,4; 36:20;37:17;45:11;50:10; 52:15;54:20;55:20;80:17</p> <p>seek (1) 49:16</p> <p>seeking (1) 64:2</p> <p>selected (1) 62:11</p> <p>self-interested (1) 10:14</p> <p>semi-classified (1) 59:10</p> <p>senior (3) 45:5,6;74:7</p> <p>sense (1) 35:21</p> <p>sensitive (3) 51:12,18;52:2</p> <p>sent (3) 6:16;52:4;58:15</p> <p>sentencing (1) 5:16</p> <p>separate (5) 22:5;25:6;50:18;74:5,6</p> <p>Sergeant (6) 30:1;31:9,15;33:15; 38:21;54:18</p> <p>serious (2) 18:8;80:17</p> <p>server (10) 16:9,11;72:7;74:5,5,6,10; 76:14,14;77:9</p> <p>servers (1) 16:3</p> <p>service (1) 16:15</p> <p>services (2) 13:5;51:14</p>	<p>session (3) 69:12,15,18</p> <p>set (2) 21:8;69:19</p> <p>setting (1) 59:10</p> <p>seven (1) 16:17</p> <p>several (5) 60:13,17;64:14;68:21; 73:18</p> <p>SF12 (1) 25:5</p> <p>Sgt (1) 31:1</p> <p>Share (9) 74:9,10,19;76:13;77:9; 79:9,16,17;80:1</p> <p>shared (1) 78:6</p> <p>SharePoint (2) 16:9;74:5</p> <p>Shaver (15) 47:4;49:5,12;50:16; 52:16;54:10;72:13;74:3; 75:3;76:2,12;77:11,21; 78:10;79:3</p> <p>Shaw (1) 4:19</p> <p>sheet (1) 73:5</p> <p>Shia (2) 40:13,14</p> <p>shoe (1) 20:3</p> <p>shot (1) 30:9</p> <p>shots (2) 74:12,18</p> <p>show (7) 16:6,14;40:17;70:10; 77:8;78:18;79:20</p> <p>showed (8) 23:18;29:13;49:3;64:1; 66:9;76:20;77:16,19</p> <p>showing (3) 16:10,11;17:1</p> <p>shows (9) 15:4;53:1;54:11;64:5; 65:11;66:5;74:2;77:13; 79:15</p> <p>side (2) 37:17;79:20</p> <p>Sidtar (1) 16:13</p> <p>SigAct (2) 15:16;31:10</p> <p>SigActs (8) 9:16;10:1;30:14;31:17; 39:12;42:6,9,19</p> <p>sight (1) 37:2</p> <p>SIGIT (1)</p>	<p>39:1</p> <p>sign (1) 26:13</p> <p>signature (1) 30:3</p> <p>signed (6) 9:21;25:4,6,15,15;37:21</p> <p>Significant (2) 9:13;39:13</p> <p>signing (1) 27:9</p> <p>similar (4) 32:10;39:16;40:4;42:18</p> <p>Similarly (1) 22:12</p> <p>simple (1) 10:7</p> <p>simply (1) 67:4</p> <p>Sintar (4) 77:6,13,14,20</p> <p>SIPR (1) 73:18</p> <p>SIPRnet (39) 11:8,9;14:6,7,10,13;15:5; 16:4,8,15,16;17:3,6,10; 38:12,14,18;39:16;45:20; 46:1,15,16;47:1,14;48:19; 50:19;53:18;54:16;63:18; 64:20;71:16;76:7;77:7; 78:1,12,14;79:1,11;80:13</p> <p>site (5) 4:13;72:18;79:9,21;80:1</p> <p>sitting (1) 47:2</p> <p>six (1) 10:3</p> <p>sixth (2) 16:2;51:17</p> <p>SJA (4) 73:19;74:1,8,19</p> <p>skills (2) 12:4;42:18</p> <p>slide (36) 18:2,2,5,10,15,19;19:3,6, 10,13,15,18;20:12,16,18; 21:6,6,8;23:7,10,11,13; 24:1,6,12;33:18,21;34:1,5, 9,14,15,18,21;35:9,16</p> <p>slides (2) 21:8;22:18</p> <p>slip (1) 68:4</p> <p>slowly (1) 72:4</p> <p>small (2) 30:6;42:20</p> <p>Smith (1) 20:2</p> <p>social (2) 22:5;35:15</p> <p>society (1) 36:2</p>
<p>S</p>			
<p>S2 (7) 30:9;31:13;36:11,12,21; 37:9;39:7</p> <p>Sadler (1) 38:21</p> <p>safe (1) 24:3</p> <p>safeguard (2) 26:10;37:19</p> <p>salutation (1) 10:2</p> <p>same (10) 9:12,15;16:9;27:17; 43:14,15;47:9;49:2,5;51:9</p> <p>sanitized (1) 36:21</p> <p>sat (1) 76:17</p> <p>saved (2) 15:16;29:19</p> <p>saw (3) 11:9;56:6,7</p> <p>scale (1) 40:12</p> <p>scene (1) 80:14</p> <p>schedule (3) 5:10,16,16</p> <p>scheduled (1) 7:7</p> <p>scheduling (1) 7:1</p> <p>SCI (1) 24:19</p> <p>SCIF (3) 36:18;37:6,7</p> <p>scoured (1) 11:7</p> <p>scrape (1) 10:5</p> <p>screen (2) 74:12,18</p> <p>SD (2) 9:15;15:15</p> <p>search (7) 39:16;40:2;46:17;49:6; 64:21;66:2,20</p> <p>searched (13) 37:4,8;47:5,7,9;49:13; 65:13;66:6,13,17,19;67:15;</p>			

software (2) 31:5;68:13	14:1;62:13;66:21	storage (1) 15:10	39:12;44:2
soldier (9) 9:19;25:13;26:8;36:4,20; 37:3,16;47:2;67:4	spies (1) 24:16	store (3) 15:11;19:13;36:14	tactics (1) 43:15
soldiers (7) 21:19;34:19,20;35:18,21; 37:8,11	spread (1) 74:16	story (1) 9:9	tag (1) 30:20
soldier's (2) 22:4;34:16	spy (1) 57:12	strike (1) 70:20	tags (1) 9:1
solely (2) 39:2;68:2	standard (2) 66:10,12	strikes (1) 75:12	talk (3) 28:7;38:10;52:19
solider (3) 37:1;39:1,2	standards (1) 19:14	strong (1) 61:21	talked (3) 22:2;57:10,12
someone's (1) 22:10	stark (1) 8:8	structure (1) 53:19	tampering (1) 28:17
soon (1) 46:3	start (1) 71:15	struggling (1) 9:19	target (1) 17:6
SOP (3) 53:12;66:14,14	started (1) 76:16	student (1) 17:19	targeted (1) 30:12
sought (3) 10:20;63:14;64:8	starting (1) 50:18	study (1) 43:6	targeting (1) 51:16
source (12) 11:7;17:9;38:19;39:1,3; 49:1,8,16,18;50:1;57:11; 68:8	starts (1) 70:13	subject (3) 8:21;33:10;72:20	task (2) 38:20;42:11
sources (3) 41:12;48:19;61:12	state (5) 8:20;9:8;16:11;48:1; 62:15	submission (1) 68:21	tasks (1) 44:5
sourcing (1) 56:18	stated (5) 17:8;26:14;49:19;58:8,17	submitting (1) 69:1	taught (5) 21:20;22:12;23:4;36:6; 51:10
Southeast (4) 40:14;48:10;57:16;65:5	statement (1) 10:10	substantive (1) 57:4	teach (1) 32:3
spanning (1) 42:19	States (56) 5:15;8:6;10:16;11:9,11, 17,21;12:3,6;13:9,13;14:1, 3;18:11;19:2,9;21:12;23:1, 17;25:10;26:18;27:21; 28:12,16,20;29:6,16;32:20; 35:3,6,10;38:19;41:2,8; 45:10,12;48:5,10;50:7,8,11; 51:9,11,17;53:14;55:6,20; 60:3;63:9,15,15;64:15; 65:5;75:11;80:15;81:2	successful (1) 15:17	team (1) 32:2
speak (1) 72:3	stating (1) 35:18	suggestions (1) 68:20	tells (1) 21:8
speaking (1) 41:10	status (1) 25:14	suite (2) 38:17;40:19	ten (2) 7:13;78:8
special (21) 8:12;20:1;26:17;27:15; 38:17;41:2,9;47:4;49:12; 50:16;52:16;54:10;72:12; 74:3;75:3;76:1,12;77:11, 21;78:10;79:3	stay (1) 58:12	summaries (2) 30:17;31:16	tend (1) 43:14
specialized (2) 11:12;32:13	steal (1) 16:19	summary (12) 41:17;47:13;50:15;52:17, 21;54:10;65:10;77:12; 78:21;79:14,17;80:3	term (7) 11:12;47:5,16,18;65:14; 66:6,6
specific (7) 13:20;23:4;37:12;39:20; 42:9;45:1;73:9	stenographer (1) 4:9	super (3) 75:8,13,17	terms (3) 17:20;49:6;73:19
specifically (14) 11:3;17:21;19:10;23:8; 24:15;29:16;35:4;38:9; 45:8;50:8;58:14;64:15; 65:7;73:18	step (3) 41:11;42:21;43:4	supplement (1) 5:12	terrorism (1) 23:5
Specification (3) 5:4;70:18,19	steps (2) 40:16;41:6	support (1) 31:3	terrorist (3) 22:17;23:5,14
specifications (2) 13:20;14:2	sticker (2) 20:3,4	sure (1) 27:7	terrorists (6) 23:12;24:16;28:17;35:7; 36:9;51:14
spectators (2) 4:10,11	stickers (1) 19:19	surrounding (1) 73:1	test (1) 24:7
speculation (1) 8:21	stipulation (3) 26:1;39:15;73:12	sworn (1) 8:4	testified (39) 17:14;22:19;25:21;27:8; 30:14,16;31:2,9,15,21;37:9, 14;39:4,15;41:18;42:4,7,17; 43:12;47:4;49:5,7,12;51:1; 54:15,18;61:11;72:13;73:7; 74:9;76:3,13;77:11,15;78:1, 10;79:3,7;80:21
spent (3)	stipulations (2) 13:16,16	systems (9) 11:14;18:18;24:5,9;38:7; 41:9,10;67:8;73:9	testifying (1) 62:13
	stood (1) 26:14	T	testimony (11) 13:15,16;26:1;39:15; 40:8;46:18;60:16;73:11,12;
		tactical (2)	

77:14;78:4 Thanksgiving (3) 46:5;65:8;70:15 theater (2) 31:6;46:3 thinking (1) 60:10 Third (3) 15:9;54:2;78:3 though (1) 20:6 thought (2) 12:15;62:3 thoughts (1) 56:3 thousands (4) 8:15;9:10;13;27:19 threat (12) 11:11;43:2;50:10;51:2; 52:14;53:5;10;54:20;20; 55:7,19;77:6 threats (2) 24:13,15 three (5) 25:1,4;42:19;50:8;63:19 throughout (3) 8:21;13:12;66:18 thus (4) 14:18;27:15;78:17;80:17 timeframe (3) 16:13;46:5;47:10 timelines (1) 30:9 times (11) 16:7;34:6;47:6,8;49:14, 15;59:12;73:18;74:16;78:8; 79:5 timing (1) 71:9 Title (1) 28:10 titled (4) 28:11;52:8;55:13;78:4 today (6) 5:20;6:4,15,20;33:8;38:3 together (4) 22:21;30:9;44:12;45:16 told (2) 31:3;59:1 tomorrow (1) 7:4 took (1) 41:5 tool (1) 40:4 tools (3) 40:19,21;41:2 top (7) 18:7;19:20;24:19;36:17; 74:14,16;80:14 topic (3) 39:21;41:12,20 topics (2)	47:8;67:2 total (1) 46:19 track (1) 78:8 tracks (1) 14:18 traditional (2) 56:10;62:10 trailer (2) 4:12,15 train (1) 40:12 trained (10) 20:10;22:16,19;24:17; 30:15;32:7;36:4;45:2,8; 58:11 training (25) 10:17;12:4;15:12,13; 17:13,16;18:3;21:4;22:18; 23:16,18,19;24:1,2,6;28:2; 29:18,20;31:2;32:1,2,13; 33:9,10,14 transaction (1) 79:21 transfer (1) 14:15 transferred (2) 71:19;72:7 translation (1) 49:10 transmission (1) 75:18 transmissions (1) 12:21 transmittal (1) 9:21 transmitted (2) 9:13;80:8 transmitting (1) 70:17 transparency (4) 59:9;60:21;61:5;64:9 transparent (1) 61:14 treated (1) 75:2 trend (4) 43:5,6,10,21 trends (2) 43:7,10 trial (3) 8:21;27:13;78:3 trip (1) 54:4 troop (1) 73:8 trophy (1) 15:17 troubled (1) 9:18 true (2) 10:11;25:2	trust (10) 8:12,13;26:10,17;27:16; 37:10,10,14,16;67:8 trusts (1) 37:18 truth (1) 57:3 try (1) 59:3 T-SCIF (6) 36:12,14,16,21;37:3;38:2 TTPs (1) 28:10 turned (1) 10:11 tweet (2) 75:11,15 tweeted (1) 71:5 twice (2) 24:7;76:21 two (14) 13:16;14:7;16:7,15;25:3, 6,15;27:9;32:14;46:15,21; 50:18;64:19;69:10 txt (1) 55:13 type (11) 10:20;12:18;18:16;34:5; 55:17;63:20;64:7;72:16; 78:9,12;80:16 types (2) 12:9;19:19 typically (1) 39:20	36:4 unit (9) 8:4;23:1;31:21;32:7; 37:15;38:6;41:18;42:14; 54:15 United (48) 5:15;8:6;10:16;11:9,11, 17,21;12:3,6;13:9,13;14:1, 2;18:11;19:2,9;21:12;23:1, 17;25:10;26:18;27:21; 29:16;32:20;35:2,6,10; 38:19;41:2,8;45:10,11;48:5, 9;50:7,8,11;51:8;53:14; 55:20;60:3;63:9,15,15; 64:15;65:4;80:15;81:1 units (2) 22:15;32:4 unit's (1) 22:13 unless (1) 37:7 unprecedented (1) 67:12 unredacted (1) 63:5 unsorted (1) 64:11 untraceable (1) 68:18 up (6) 9:9;31:11;40:7;70:3; 73:10;78:18 updates (1) 49:12 uploaded (2) 71:20;72:8 upon (1) 43:9 usable (1) 41:21 USC (2) 5:5;25:19 use (14) 8:17;22:14,21,21;28:17; 30:15;34:7;35:2,21;44:16; 45:9;52:9;53:8,13 used (26) 4:16;11:1;12:5;14:14; 16:19;22:1,20;32:20;33:1; 38:7,11,12,16;39:10,20; 40:3;42:15;48:19;49:2,2; 51:10;52:12;60:1,18;61:14; 68:10 useful (2) 13:18;43:16 user (3) 17:3;78:11,19 uses (1) 68:13 USFI (1) 16:19 using (6) 22:18;46:4,16;49:6;
		U	
		ultimately (5) 6:3;12:5;21:11;24:11; 31:13 un (1) 68:18 unable (1) 78:17 unauthorized (1) 51:12 uncertain (2) 25:13,16 unclassified (3) 19:20;49:10;53:13 under (9) 6:12;18:12;19:2,18; 25:19;51:6;59:13;73:6; 78:11 understood (7) 19:21;21:19;27:7,21; 29:12;36:5;45:3 undisputed (1) 71:7 unfeathered (1) 10:14 uniform (1)	

64:20;76:10 utilities (1) 60:7 utility (1) 60:15	volume (2) 15:2,4 volumes (1) 33:5 volumestxt (1) 53:17 voluminous (1) 11:16 voluntarily (2) 26:13;27:9 vulnerability (1) 55:1	8:14 Whyte (1) 4:6 WickiLeaks (103) 8:18;9:14;10:1,19,21; 11:2,3,8,10;12:13,16;14:16; 15:12;16:6;17:4;28:6; 32:21;33:6;45:14;46:2,10, 10,17;47:6,11,16,18;48:2,4, 14,20;49:7,13;50:6,10,14; 51:3,6,18;52:3,4;53:5,6,16; 54:20;55:2,12;56:3,6,7,15, 21,21;57:19;58:3,4,6,8,11, 15;59:5,17,17,21;61:4,18, 19,20;62:3,5,9,14,19;63:2,4, 10,13,14,20;64:2,5;65:12; 66:5,9;67:3,17,19;68:1,8, 10,12,17,20;70:14,17;71:1, 5,14,20;72:1,8;75:11,15 WickiLeaks' (2) 50:1;56:9 WickiLeaksorg (1) 55:6 widely (1) 29:1 Wikipedia (1) 68:18 willing (1) 72:1 Windows (4) 72:15,15;78:8;79:6 wipe (1) 76:10 wiped (2) 14:17;76:9 within (11) 8:12;26:15;34:11;37:15; 39:8;53:14;55:8;71:15; 72:14;74:19;77:19 without (3) 47:1;55:10;58:5 witness (1) 5:7 witnessed (1) 71:11 witnesses (6) 5:10,16;13:15;17:14; 38:5;73:7 WMD (1) 72:15 WMV (4) 78:9,12,19;79:12 word (1) 60:19 words (5) 9:10;12:14;22:2;46:4; 56:16 work (4) 12:8;32:15;44:21;81:7 WorkChat (1) 40:4 worked (4) 30:16;36:12,16;38:1	working (1) 48:13 world (11) 11:15;14:9,14;41:8; 48:17;52:5;57:20;59:17; 60:2;68:2;71:14 Worldwide (4) 9:6;21:3,15;49:11 worth (1) 9:10
V	W	Y	Z
vaguely (1) 67:6 valuable (1) 32:16 values (1) 61:13 varies (1) 43:19 various (1) 41:12 vehicles (1) 35:2 venerable (1) 54:21 versions (1) 64:10 versus (1) 43:19 via (1) 8:17 video (36) 15:21;20:2,7,7;58:17,18; 70:17,20;71:4,7,16,17,18, 19;72:6,7,14,16,17;73:7,12; 75:19;76:20;77:3,5;78:4,16, 16;79:10;80:5,7,10,14,16, 21;81:2 videos (17) 35:15;65:12,13,14,17,18, 20;66:1;73:6;74:9,20; 75:12;76:4,4,15;79:9;80:10 view (2) 31:18;61:21 viewed (3) 50:17;78:18,19 violate (2) 27:1,5 violated (1) 27:14 violating (1) 27:15 violation (1) 25:18 violations (2) 27:12;51:10 violently (1) 59:3 visitor (1) 74:21 visualize (1) 41:17 vital (1) 24:3 void (1) 77:17	waged (1) 28:1 walk (1) 12:17 wantonly (1) 13:3 wants (1) 59:3 war (3) 8:4;14:13;28:1 warfare (1) 29:3 Washington (1) 59:12 watch (1) 71:17 watched (1) 58:18 way (5) 11:1;19:13;43:10;57:14; 61:14 weapon (2) 18:18;73:9 weapons (3) 28:12,13;35:1 web (11) 16:5;20:20;21:1,15; 48:17;52:9;61:16;74:12,14; 75:13;79:6 website (16) 5:20;28:17;49:8,11; 50:15;51:20;52:3;53:7; 55:3;64:6;68:20;74:1,2; 75:1;76:18;79:18 websites (2) 23:14;74:3 week (2) 9:12;46:20 weekend (1) 7:4 weekly (1) 42:16 weeks (7) 8:12;16:7;46:15;47:1; 50:19;64:19;71:15 whenever (1) 21:20 wholesale (1)	year (1) 42:19 years (2) 23:14;68:5 yesterday (1) 6:13 York (1) 59:12	zip (4) 72:14;78:17;79:10,12 zone (1) 8:4
		0	09 (5) 46:14,14;50:19;65:3; 68:10 0930 (1) 7:9
		1	1 (10) 16:7;18:2;33:18;47:6; 50:19;71:18;72:6;76:16,19; 80:8 10 (12) 18:15;23:14;35:9;42:2,3; 56:19;64:17;79:7,14,18; 80:2,2 10:45 (1) 7:16 100 (2) 23:15;47:6 101 (1) 66:16 108 (1) 76:15 109 (3) 50:3;64:11,17 11 (8) 18:19;24:12;28:4;35:16; 57:13,15;70:18,19 110 (1) 64:11 112 (1)

66:16	2000 (1)		4:8
114 (1)	70:15	3	58 (1)
23:20	2003 (1)		77:18
115 (1)	66:12	3 (2)	59 (1)
65:20	2007 (1)	34:1;55:5	26:20
116 (1)	58:18	30 (4)	
65:21	2008 (8)	54:6;58:9;65:2;66:7	6
119 (1)	24:1;26:2;32:1;33:19;	31 (3)	
16:6	35:9;17;36:5;52:8	14:18;19:10;76:7	6 (3)
12 (3)	2009 (34)	32 (3)	5:5;17:17;34:14
5:5;54:11,16	8:3;16:1,1,7;24:1;32:8;	65:15,18;75:10	60 (1)
12:00 (1)	46:5;47:7;54:7;58:18;65:8,	33 (1)	27:3
70:7	11,15;66:4,7,12;67:1,1,5;	58:20	614 (2)
123 (1)	71:3,19,21;72:6,9;73:15,16,	35 (3)	5:3,18
56:13	17,17;75:7,19;76:16,19;	4:10;17:14;24:20	615 (1)
127 (2)	80:8,9	38 (1)	5:6
53:17;55:14	2010 (26)	19:13	616 (2)
128 (3)	9:12;14:18;16:13;47:8;	380-5 (1)	5:9,14
78:20;79:2,15	48:12;49:1;50:20;53:2;	18:4	617 (1)
129 (2)	54:3,13;60:13;62:12;71:6;	3C (2)	5:12
79:14,17	75:11,14;76:7,8,21;77:1,5,	54:4,11	63 (2)
13 (4)	9,19;78:2;79:7,14,19	3rd (1)	50:15;66:8
33:18;35:9,17;36:5	2013 (3)	46:19	641 (2)
130 (2)	5:3,6,9		5:5;25:20
16:21;17:1	21 (1)	4	65 (1)
1330 (2)	19:6		73:3
81:7,9	210 (3)	4 (2)	7
139 (1)	27:6;36:11;46:20	5:4;34:5	
49:3	216 (1)	4,000 (1)	7 (12)
14 (4)	23:7	23:15	18:5;23:19,21;24:6,13;
4:11;19:3;53:2;54:12	219 (1)	40 (2)	26:1;34:15,18;50:20;54:3;
15 (14)	23:10	14:7;58:17	57:11;76:10
16:1,1;20:4;66:18;69:11,	22 (1)	41 (1)	71 (1)
20;70:2,3;71:3,20;72:9;	14:7	19:15	20:12
75:6,19;80:9	221 (1)	42 (1)	7-100.1 (1)
154 (1)	23:11	68:7	28:20
66:1	223 (1)	43 (2)	7-100.4 (1)
155 (1)	23:13	54:9;55:5	29:6
66:2	23 (6)	44 (1)	72 (1)
15-6 (1)	52:8;77:1,5,9,19;78:2	66:7	20:16
81:3	24 (4)	45 (2)	73 (1)
16 (1)	5:3;28:7;46:7;67:5	50:21;51:4	20:18
5:5	25 (6)	46 (3)	7-903 (1)
160 (1)	5:6,9;33:17,18;47:8;	51:1;66:8;71:2	25:19
13:13	49:14	470 (1)	
161 (3)	250,000 (1)	66:20	8
77:11,12,18	62:15	474 (1)	
17 (1)	251,287 (1)	66:20	8 (9)
66:1	63:5	48 (1)	4:9;5:5;18:10;34:21;
18 (2)	26 (2)	19:18	65:2;66:15;71:5;75:11,14
5:5;25:19	54:6;58:13		80 (2)
19 (2)	272 (1)	5	13:15;62:14
16:18;53:2	62:16		802 (1)
2	28 (6)	5 (8)	6:19
	65:2,7,14,15,18;76:21	17:17;34:9;49:21;53:16;	81 (7)
2 (6)	283 (1)	54:2;59:4,9;68:6	47:12,12,15;65:1,10,15;
5:5;24:1;33:21;57:8;	66:3	51 (1)	73:20
70:18,19	29 (6)	22:18	84 (1)
20 (2)	46:14,14;65:2,14;66:7;	52 (3)	50:17
49:1,14	73:16	18:2;20:10;21:7	85 (3)
2-0 (1)	2nd (1)	525-13 (1)	52:17,21;54:10
28:11	46:19	28:15	
		54 (1)	

9			
9 (6) 35:4;46:6;56:14;65:17, 20;73:17 9:20 (1) 4:7 91 (3) 74:11,14,18 917 (1) 6:12 99 (1) 52:10			